目次

第 4 章 インストールと設定

はじめに

このたびは弊社製品をご購入いただき、誠にありがとうございます。
このマニュアルは、パソコンまたはワークステーション本体に搭載されているセキュリティチップ、指紋センサー、FeliCa 対応リーダ／ライタ、スマートカードリーダ／ライタ、またはスマートカードホルダー（以降、認証デバイス）の基本的な取り扱い、認証デバイスをお使いになるためのソフトウェアのインストール、および設定と使い方について説明しています。
お使いになる前に、このマニュアルおよびパソコンまたはワークステーション本体のマニュアルをよくお読みになり、正しくお使いいただきますようお願いいたします。

2006 年 4 月

■ セキュリティ機能について

セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。弊社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。

SMARTACCESS のマニュアルについて

認証デバイスをお使いになるためのソフトウェア「SMARTACCESS」について、次のマニュアルを用意しております。目的に合わせてお読みください。

■ SMARTACCESS ファーストステップガイド（認証デバイスをお使いになる方へ）

このマニュアルです。
認証デバイスのドライバインストール手順、設定手順と取り扱い方、および SMARTACCESS のインストール、アンインストールと初期設定手順を説明しています。

■ SMARTACCESS/Premium リファレンスガイド、または SMARTACCESS/Basic リファレンスガイド

□ 機能編

SMARTACCESS の代表的な機能と使い方について、目的別に説明しています。

□ ツール編

SMARTACCESS のメニューに沿って、機能全般について説明しています。

□ カスタマイズ編（SMARTACCESS/Premium のみ）

SMARTACCESS をインストールした時点で標準設定以外に設定して運用するために必要な準備、およびインストール方法について説明しています。

『SMARTACCESS/Premium リファレンスガイド』はすべて、「SMARTACCESS/Premium」CD-ROM に格納されています。
『SMARTACCESS/Basic リファレンスガイド』はすべて、パソコンまたはワークステーション本体に添付の「ドライバーズディスク」に格納されています。

このマニュアルの表記

■本文中の記号

本文中に記載されている記号には、次のような意味があります。

記号	意味
重要	お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページや参照マニュアルを示しています。

■キーの表記と操作方法

本文中のキーの表記は、キーボードに書かれているすべての文字を記述するのではなく、説明に必要な文字を次のように記述しています。

例：【Ctrl】キー、【Enter】キー、【→】キーなど

また、複数のキーを同時に押す場合には、次のように「＋」でつないで表記しています。

例：【Ctrl】＋【F3】キー、【Shift】＋【↑】キーなど

■連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：「スタート」ボタンをクリックし、「プログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「プログラム」→「アクセサリ」の順にクリックします。

また、本文中の操作手順において、操作手順の類似しているものは、あわせて記述しています。

例：「スタート」ボタン→「(すべての) プログラム」→「アクセサリ」の順にクリックします。

■画面例およびイラストについて

表記されている画面およびイラストは一例です。お使いの機種や OS、Web ブラウザなどの環境、またインストールされている認証デバイスにによって、画面およびイラストが若干異なることがあります。

■製品の呼び方

本文中の製品名称を、次のように略して表記します。

<table>
<tr><th>製品名称</th><th colspan="3">本文中の表記</th></tr>
<tr><td>認証デバイスを搭載した FMV シリーズ</td><td>パソコン本体</td><td colspan="2" rowspan="2">コンピュータ</td></tr>
<tr><td>認証デバイスを搭載した CELSIUS シリーズ</td><td>ワークステーション本体</td></tr>
<tr><td>セキュリティチップ</td><td colspan="2">セキュリティチップ</td><td rowspan="5">認証デバイス</td></tr>
<tr><td>FMV シリーズ内蔵スライド方式指紋センサー</td><td colspan="2">指紋センサー</td></tr>
<tr><td>FeliCa 対応リーダ／ライタ</td><td colspan="2" rowspan="3">リーダ／ライタ</td></tr>
<tr><td>スマートカードリーダ／ライタ</td></tr>
<tr><td>スマートカードホルダー</td></tr>
<tr><td>SMARTACCESS に対応した FeliCa 対非接触 IC カード（FeliCa 対応非接触応 IC カード（SMARTACCESS 専用）を含む）</td><td>IC カード（FeliCa 方式）</td><td colspan="2" rowspan="2">カード</td></tr>
<tr><td>スマートカード</td><td>スマートカード</td></tr>
<tr><td>SMARTACCESS/Premium</td><td rowspan="2">SMARTACCESS</td><td colspan="2" rowspan="2">本製品</td></tr>
<tr><td>SMARTACCESS/Basic</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td>Windows XP Professional</td><td rowspan="3">Windows XP</td><td rowspan="6">Windows</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td><td>Windows XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® XP Tablet PC Edition 2005</td><td>Windows XP Tablet PC Edition 2005</td></tr>
<tr><td>Microsoft® Windows® 2000 Professional</td><td colspan="2">Windows 2000</td></tr>
<tr><td>Microsoft® Windows Server ™ 2003, Enterprise Edition</td><td>Windows Server 2003</td><td rowspan="2">Windows Server</td></tr>
<tr><td>Microsoft® Windows® 2000 Server</td><td>Windows 2000 Server</td></tr>
<tr><td>Microsoft® Internet Explorer</td><td colspan="3">Internet Explorer</td></tr>
<tr><td>Microsoft® Outlook® Express</td><td colspan="3">Outlook Express</td></tr>
<tr><td>Microsoft® Office Outlook® 2003</td><td colspan="3">Outlook</td></tr>
<tr><td>Microsoft® Office Word 2003</td><td colspan="3">Word</td></tr>
<tr><td>Netscape® または Netscape® Communicator</td><td colspan="3">Netscape</td></tr>
<tr><td>FENCE-G® V4 以降</td><td colspan="3">FENCE-G</td></tr>
</table>

用語集

用語	説明
Active Directory	Windows Server のディレクトリ サービスで、Windows Server の分散ネットワークの基盤となるものです。
FENCE-G	コンピュータの各種ポートの読み書きを制御できるソフトウェアです。
PIN（Personal Identification Number）	IC カード（FeliCa 方式）やスマートカードを使うときのパスワードの一種です。
Portshutter	コンピュータの各種ポートを使用制限できるソフトウェアです。

用語	説明
Security Platform（Infineon TPM Professional Package）	セキュリティチップを使用するために必要なユーティリティです。
SMARTACCESS アカウント	SMARTACCESS を利用するためのアカウント情報です。ユーザー名とパスワードを登録します。
Systemwalker	セキュリティ管理、ジョブ管理などを行う統合運用管理ソフトウェアです。本製品と連携することで、利用イベントの集中管理やファイル暗号化ができます。
Windows ログオン情報	認証デバイスに登録する、Windows にログオンするときのユーザー名、パスワード、ドメイン名などです。
アプリケーションログオン情報	認証デバイスに登録する、アプリケーションや Web サイトにログオンするときのユーザー名、パスワードなどです。
暗号鍵	情報を暗号化または復号するときに使用する、特定のデータです。
オブジェクト	Active Directory の用語で、ユーザーやコンピュータ、組織単位（OU）を指します。
カード IDm	IC カード（FeliCa 方式）のシリアル番号です。カード製造時に一意に割り当てられます（カードに刻印された番号とは異なります）。
カード抜き取り	IC カード（FeliCa 方式）またはスマートカードをセットした状態から外す操作です。
管理者	本製品を管理する人（セキュリティポリシーを設定したり、管理したりする人）です。 通常、Windows アカウントは管理者（Administrators）権限です。
管理者 PIN	管理機能を利用する場合に必要となる PIN です。
管理者権限カード	カード管理リストで、管理者属性が設定されているカードです。
機器監査	あらかじめ機器構成を登録し、Windows 起動時の機器構成と比較することで、機器構成が変更されていないかを監査する機能です。
機器構成	BIOS 設定のハードウェア構成やメモリスロットの構成など、使用しているコンピュータのハードウェア構成です。
コントロール ID	アプリケーションの各入力フィールドやボタンに割り振られている、個別のIDです。フィールドIDとも表記します。
証明書	本人を証明する電子証明書のことです。本製品では、Windows ログオンや Web サーバーへのアクセスにお使いになれます。
所有者	IC カード（FeliCa 方式）やスマートカードなど、持ち運び可能な認証デバイスを所有する人です。
所有者 PIN	通常使用する PIN です。
シングルサインオン	Windows にログオンするときに 1 回認証することで、アプリケーションにログオンするときにログオン情報を自動で入力する機能です。一度認証に成功すると、以降パスワードや指紋の入力なしで認証します。

用語	説明
セキュリティチップ	TPM（Trusted Platform Module）と呼ばれるセキュリティ用の専用ハードウェアチップです。 セキュリティチップは内部に暗号鍵を保持し、アプリケーションで使用するパスワードなどを暗号化します。セキュリティチップに保持された暗号鍵は外部に出す方法がありませんので安全に管理できます。
セット	IC カード（FeliCa 方式）を FeliCa 対応リーダ／ライタに接触させ続ける操作です。
組織単位（OU）	Active Directory のユーザーやコンピュータをまとめるための入れもののことです。ユーザーやコンピュータを組織化する場合などに利用します。
タッチ	IC カード（FeliCa 方式）を FeliCa 対応リーダ／ライタに一時的に接触させる操作です。
認証デバイス	認証を行う手段や装置です。 本製品では、セキュリティチップ、指紋センサー、FeliCa 対応リーダ／ライタ、スマートカードリーダ／ライタ、およびスマートカードホルダーを指します。
バイオ認証装置	指紋を利用して認証する認証サーバーです。
バイオパスワード	指紋を登録するときや、指紋でのログオンを回避するときに使用するパスワードです。
パスワード入力画面情報／パスワード入力画面情報ファイル	ログオンしたいアプリケーションや Web サイトのパスワード入力画面の情報を格納しているファイルです。
ポーリング	リーダ／ライタに IC カード（FeliCa 方式）やスマートカードなどをタッチしたり、抜き取ったりしたときに、コンピューターのロックや強制ログオフなどを行い、コンピュータを不正な使用から保護することです。
ユーザーキーパスワード	セキュリティチップを使用する際に入力するパスワードです。セキュリティチップを使用するユーザーごとに設定します。 基本ユーザーパスワードとも表記します。
ユーザー情報	Windows ログオン情報およびアプリケーションログオン情報などの認証用の情報のことです。例えば、ユーザー名やパスワード、指紋、PIN などを指します。
利用者	本製品を管理者のもとで使う人です。
連携アプリケーション	SMARTACCESS の機能を拡張させるために、連携できる他製品を指します。

商標および著作権について

第 1 章

お使いになる前に

この章では、認証デバイスや SMARTACCESS をお使いになる前に確認していただくことを説明しています。

1 動作環境

認証デバイスや SMARTACCESS をお使いになる前に、次の条件を確認してください。

重要

- コンピュータに搭載されている認証デバイスをお使いになれます。カスタムメイドで選択していない場合など、機種によってはお使いになれない認証デバイスもあります。

SMARTACCESS

■ 対応機種／ OS

認証デバイスが搭載されている FMV シリーズ、CELSIUS シリーズ／ Windows XP、Windows 2000

注：ハードディスク容量に 50MB 以上の空きがあること

POINT

- WEB ページをご覧になるためのアプリケーションとして、Internet Explorer 6.0 以降または Netscape 4.78 ／ 7.0 以降が必要です。
- セキュア E-mail をお使いになるには、Outlook 2000 ／ 2002 以降、Outlook Express 6.0 以降、または Netscape 4.78 ／ 7.0 以降が必要です。
- Word マクロへの署名を利用するには、Word 2000 ／ 2002 以降が必要です。
- VeriSign 証明書を利用するには、Internet Explorer 6.0 または Netscape 4.78 ／ 7.0 が必要です。
- SMARTACCESS での、アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求機能は、Netscape ではお使いになれません。

■ SMARTACCESS がサポートする認証デバイス

□ SMARTACCESS/Premium

認証デバイス	製品名
セキュリティチップ	FMV シリーズ、および CELSIUS シリーズ内蔵のセキュリティチップ
指紋センサー	FMVシリーズ内蔵スライド方式指紋センサー
FeliCa リーダ／ライタ	FMV-LIFEBOOK 内蔵の FeliCa リーダ／ライタ
スマートカードリーダ／ライタ	FMV シリーズ、および CELSIUS シリーズ内蔵のスマートカードリーダ／ライタ FMV-LIFEBOOK カスタムメイド、およびオプションのスマートカードホルダー

□ SMARTACCESS/Basic

認証デバイス	製品名
セキュリティチップ	FMV シリーズ、および CELSIUS シリーズ内蔵のセキュリティチップ
指紋センサー	FMVシリーズ内蔵スライド方式指紋センサー
スマートカードリーダ／ライタ	FMV シリーズ、および CELSIUS シリーズ内蔵のスマートカードリーダ／ライタ FMV-LIFEBOOK カスタムメイド、およびオプションのスマートカードホルダー

第 2 章

認証デバイスについて

認証デバイスをお使いになるための注意事項や基本的な取り扱い方について説明しています。

1 セキュリティチップ

概要

■セキュリティチップとは

セキュリティチップは、TCG 注1 の仕様に基づいた TPM 注2 と呼ばれる IC チップで TCG セキュリティの基本機能を提供します。セキュリティチップを搭載したコンピュータは、ソフトウェアによる攻撃および物理的な攻撃からデータを保護し、より強固なセキュリティを実現します。

注 1: TCG は Trusted Computing Group の略称です。
TCG は、信頼性と安全性を持った新しいコンピュータをつくるためのオープンな業界仕様を策定する団体です。
(https://www.trustedcomputinggroup.org/)

注 2: TPM は Trusted Platform Module の略称です。

■セキュリティチップの機能

セキュリティチップは、各ユーザに固有の鍵を生成し、証明書を管理します。この鍵と証明書を用いることにより、セキュリティチップは暗号化や認証を行います。セキュリティチップ内に保有する鍵は、取り出すことが不可能なため鍵の解読ができません。そのため暗号化されたデータや認証は安全に行われます。ユーザはこの鍵と証明書を利用するためのパスワードを設定します。

■セキュリティチップの利用

セキュリティチップを利用するために、次のソフトウェアおよび証明書を使用します。

・Infineon TPM Professional Package（Infineon Security Platform）ユーティリティ
・SMARTACCESS
・VeriSign 証明書

これらのソフトウェアおよび証明書により、次のことが行えるようになります。

□ IEEE802.1x 認証ファイルの管理

IEEE802.1x にて利用する証明書をセキュリティチップで管理することができます。

□ ファイルとフォルダの暗号化 -EFS（Encrypting File System）

ユーティリティでファイルとフォルダの暗号化を設定することにより、EFS による暗号化に利用される鍵をセキュリティチップで安全に保管します。

重要

▶ EFS を利用するには、ハードディスクが NTFS でフォーマットされている必要があります。
▶ Windows XP Home Edition では、EFS は利用できません。
▶ ハードディスク全体またはボリューム全体を、暗号化することはできません。
▶ 次のようなフォルダは暗号化しないでください。セキュリティチップが利用できなくなったり、コンピュータが起動できなくなったりする場合があります。
・Windows の起動に必要なファイルのあるフォルダ（C:¥Windows など）

・ユーザー情報の入ったフォルダ（C:¥Document and Settings¥ ＜ユーザー名＞など）
・ソフトウェアがインストールされているフォルダ（C:¥Program Files など）

- セキュリティチップのバックアップファイルを保存したフォルダは暗号化しないでください。セキュリティチップが利用できなくなる場合があります。

□ セキュア E-Mail

ユーティリティで E-Mail の保護を設定することにより、E-Mail の暗号用の証明書をセキュリティチップで安全に管理します。

□ Word マクロへの署名

ユーティリティでセキュリティ機能を設定することにより、Word マクロへの署名をセキュリティチップで安全に保護します。

□ Windows ログオンにセキュリティチップを利用する

SMARTACCESS による Windows ログオンを設定することにより、Windows ログオン時のパスワードをセキュリティチップで安全に保存することができます。

□ コンピュータの不正なハードウェアの変更の検出

SMARTACCESS の「機器監査」機能を利用すれば、Windows ログオン時コンピュータの機器構成のチェックを行います。ハードウェア構成または設定が不正に変更されていることを検出した場合は、Windows ログオンを許可しないようにすることができます。

□ VeriSign 証明書の利用

セキュリティチップと連携した VeriSign 発行の証明書を、登録した日から 1 年間無料で利用できます。これを利用することにより、例えばセキュア E-mail を利用する場合などは、VeriSign 認証局に証明された証明書を利用できるため、より安全なデータを送受信することができます。

POINT

- VeriSign 証明書は、セキュリティチップのユーティリティをインストールし、設定を完了して利用可能にしてからインストールを行ってください。インストールについては、それぞれ次のファイルをご覧ください。
  ・「SMARTACCESS/Premium」をお使いの場合
  　添付の「SMARTACCESS/Premium」CD-ROM 内にある「¥ifxsw20¥versign.txt」
  ・「SMARTACCESS/Basic」をお使いの場合
  　添付の「ドライバーズディスク」内にある「¥other¥ifxsw20¥versign.txt」
- VeriSign 証明書は、登録した日から 1 年間利用できます。それ以降は、E-mail などで証明書を利用することはできません。ただし、古いメールなどで利用していた場合には、読むことのみ可能です。
- 1 年間の利用期間終了後もご利用を希望の場合は、弊社担当営業員までご連絡ください。その場合有料による継続となります。

■ セキュリティチップの管理

セキュリティチップには、セキュリティチップの管理を行う「所有者」とセキュリティチップを使用する「ユーザ」を登録します。
所有者およびユーザは次の鍵および証明書やファイルを作成・利用します。

POINT

▶ SMARTACCESS では次のようにお使いになることをお勧めします。

SMARTACCESS	セキュリティチップ
管理者	所有者
利用者	ユーザ

□「所有者」が管理するもの

所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。この鍵はセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。所有者パスワードは忘れないよう注意してください。

自動バックアップファイルと復元用トークン

セキュリティチップで管理しているすべての鍵や証明書のバックアップを行います。バックアップはスケジュールを設定することにより定期的に行うことができます。
セキュリティチップが故障しても、新しいコンピュータでこのファイルを用いて復元することにより、以前利用していた暗号化ファイルなどが利用できるようになります。
自動バックアップファイルは、トークンにより暗号化されています。自動バックアップファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

パスワードリセットファイルとリセットトークン

ユーザーがセキュリティチップのパスワードを忘れた場合に備えて、前もってパスワードリセット用のファイルを作成しておくことで現状のパスワードを新規パスワードに変更することができます。所有者は事前にパスワードリセットの設定を行い、必要に応じてユーザのパスワードを設定し直します。
パスワードリセットファイルは、トークンにより暗号化されています。パスワードリセットファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

□「ユーザ」が管理するもの

ユーザーキーとユーザーキーパスワード

ユーザはセキュリティチップを利用する場合、ユーザーキーを作成します。このキーはセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。キーを紛失した場合は、それ以前に暗号化していたデータやファイルなどを再び利用することができなくなります。管理には注意してください。また、パスワードを忘れた場合も、キーが利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう注意してください。

使用上のご注意

■セキュリティチップで利用する鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイルなどは利用できなくなることがありますので注意してください。またこれらの鍵を利用する場合はパスワードが必要です。パスワードを正しく入力しないと鍵が利用できないため、紛失時と同様に暗号化されたファイルなどが利用できなくなります。

■セキュリティチップ利用についてのご注意

- セキュリティチップで使用するソフトウェアをインストールするときには、コンピュータ本体またはネットワーク上のコンピュータに、CD-ROM ドライブが搭載または接続されている必要があります。
- セキュリティチップで鍵を生成する場合、数分かかることがあります。
- コンピュータ本体の修理・保守を依頼する場合は、SMARTACCESS による Windows ログオンを解除してください。
  SMARTACCESS による Windows ログオンを解除していない場合、修理・保守ができないことがあります。SMARTACCESS による Windows ログオンを解除するには、次の手順を行ってください。
  1. SMARTACCESS をインストールしたユーザで Windows にログオンします。
  2. 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。
     「環境設定」が表示されます。
  3. 「ログオン認証」－「Windows ログオン」の順にクリックします。
  4. 「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。

  また、パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定し、任意のパスワードに変更してから「SMARTACCESS による Windows ログオン」を使用しない設定にしてください。
- コンピュータ本体の修理・保守が行われた場合には、セキュリティ機能が解除されていることがあります。その場合には環境の再構築が必要となります。正しく再構築がされない場合、暗号化されたファイルやメールが復元できなくなる場合があります。

■セキュリティチップの運用上の注意

セキュリティチップを利用するための環境設定が完了すると、ファイルやフォルダの暗号化、メールの証明書の管理などがより安全な環境で運用することができるようになります。ただし故障や修理などでコンピュータ本体の設定が変更された場合、セキュリティチップにより保護された情報が利用できなくなることがあります。
これらの場合に備えて、次の点に注意して運用してください。

POINT

- 次のような場合に、セキュリティチップが利用できなくなる場合があります。
  - ・セキュリティチップの故障

・ハードディスクのリカバリ
・コンピュータの部品の交換

□ 定期的にセキュリティチップの鍵のバックアップを行う

必ずセキュリティチップによって管理されている鍵の定期的なバックアップの設定を行ってください。
バックアップファイルを紛失したり、パスワードを忘れたりすると、セキュリティチップが利用できなくなります。バックアップファイルやその時に設定したパスワードは、紛失したり忘れたりしないよう注意して管理してください。
バックアップの方法については、「バックアップについて」(→ P.21) をご覧ください。

重要

▶ セキュリティチップの機能をすべてお使いになると、次のファイルとパスワードが生成されます。ご利用の設定によって、このうち一部が生成される場合があります。

利用者	ファイル	ファイル名
所有者	所有者パスワード	
	システム復旧ファイル	spsystembackup.xml
	緊急時復元用トークン	spemrectoken.xml
	緊急時復元用トークンパスワード	
	パスワードリセットファイル	sppwdresetsecret.xml
	パスワードリセットトークン	sppwdresettoken.xml
	パスワードトークンパスワード	
	(基本) ユーザーパスワード	
ユーザ	(基本) ユーザーパスワード	
	パスワードリセットトークン	sppwdresetsecret.xml
	パスワードトークンパスワード	

▶ 復元作業は、パスワードの入力などが必要なため、弊社で行うことはできません。「リストアについて」(→ P.21) をお読みになり、注意して復元してください。

□ 機器監査を行っている場合は、修理またはハードウェア変更を行う前に SMARTACCESS による Windows ログオンを一時的に解除する

SMARTACCESSによるWindowsログオンを使用する設定にして機器監査を行っている場合、修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。
必ず SMARTACCESS による Windows ログオンを使用しない設定に変更してください。変更方法については、「コンピュータの修理について」(→ P.23) をご覧ください。

■バックアップについて

セキュリティチップで保護された環境に何らかの変更があった場合でも、引き続き以前の環境を利用するためには鍵のバックアップを行っておく必要があります。
所有者でログオンした時に、通知領域から表示される内容により、手順に従いバックアップを行ってください。
所有者はセキュリティチップのバックアップと各ユーザのバックアップを行う必要があります。
各ユーザでバックアップを行う必要はありませんが、復元を行った後、ユーザーキーパスワードを入力する必要があります。

重要

- バックアップの方法については、次のマニュアルをご覧ください。
  - ・SMARTACCESS/Premium をお使いの場合
    『SMARTACCESS/Premium リファレンスガイド　ツール編』の「オプションツール」－「バックアップツール」
  - ・SMARTACCESS/Basic をお使いの場合
    『SMARTACCESS/Basic リファレンスガイド　ツール編』の「オプションツール」－「バックアップツール」
- バックアップは、セキュリティチップの中の鍵を取り出して保存することではありません。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。
- 手順は、セキュリティチップの鍵についてバックアップを行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESS の設定については行われません。必要に応じて別途バックアップを行ってください。
  SMARTACCESS のバックアップについては、『SMARTACCESS/Premium リファレンスガイド　ツール編』、または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「オプションツール」－「バックアップツール」をご覧ください。

■リストアについて

リストアは、セキュリティチップで保護された環境に変更があった場合、以前の環境を引き続き利用するための作業です。
所有者はセキュリティチップのリストアを行います。
ユーザは、リストアを行う必要はありませんが、所有者がリストアを行った後にユーザーキーパスワードを入力する必要があります。

重要

- リストアの方法については、次のマニュアルをご覧ください。
  - ・SMARTACCESS/Premium をお使いの場合
    『SMARTACCESS/Premium リファレンスガイド　ツール編』の「オプションツール」－「バックアップツール」
  - ・SMARTACCESS/Basic をお使いの場合
    『SMARTACCESS/Basic リファレンスガイド　ツール編』の「オプションツール」－「バックアップツール」
- リストアは、セキュリティチップの所有者パスワードによって保護されています。そのため、リストアはセキュリティチップの所有者が行う必要があります。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。

■機器監査について

SMARTACCESS で「SMARTACCESS による Windows ログオン」を設定しておくと、コンピュータの電源を入れたときやコンピュータを再起動したときにハードウェアの変更を検出すると、Windows のログオンを禁止することができます。これにより、ユーザが気づかないうちに（帰宅時など）ハードウェアを変更されても、検出することができます。
なお、不正にコンピュータの設定が変更されたときだけでなく、修理により設定が変更された場合でも機器監査変更が検出されることがあります。修理に出す前に「コンピュータの修理について」（→ P.23）をご覧になり、前もって設定を変更できるようにしてください。
ハードウェアの変更については次の項目が検出されます。

重要

- 機器監査の設定方法については、次のマニュアルをご覧ください。
  - SMARTACCESS/Premium をお使いの場合
    『SMARTACCESS/Premium リファレンスガイド　機能編』の「Windows ログオン」－「機器監査」
  - SMARTACCESS/Basic をお使いの場合
    『SMARTACCESS/Basic リファレンスガイド　機能編』の「Windows ログオン」－「機器監査」
- 次の変更を行う前に SMARTACCESS の「機器監査」をオフにし、変更後、再度「現在の機器構成情報の登録」を行う必要があります。
- FMV-W シリーズの場合、ハードウェアや BIOS 設定の変更を元に戻しても、機器監査の状態が元に戻らないことがあります。そのため、誤って変更してしまったり、変更後に機器監査の再登録を行わなかったりすると、Windows にログオンできなくなります。その場合は、機器構成を登録し直す必要があります。

POINT

- ハードウェアの変更については、休止状態からの復帰時にも確認されます。

□ BIOS 設定変更

BIOS でハードウェア構成が変更された場合に、機器監査で通知されます。

□ メモリ構成の変更

メモリスロットの構成に変更があった場合に、機器監査で通知されます。

□ ハードディスクドライブ構成の変更（FMV-W シリーズの場合）

ハードディスクドライブの構成に変更があった場合に、機器監査で通知されます。

□ PCI スロット、グラフィックボードの変更（FMV-ESPRIMO、FMV FA パソコン、および CELSIUS シリーズの場合）

PCI スロットの構成およびグラフィックボードを変更した場合に、機器監査で通知されます。

□ モバイルマルチベイ／マルチベイの変更（FMV-LIFEBOOK の場合）

モバイルマルチベイまたはマルチベイを変更した場合に、機器監査で通知されます。

□ USB デバイスの変更

USB ポートに USB メモリなどのストレージデバイスを接続した場合に、機器監査で通知されます。

POINT

- USBデバイスの変更を検出するには、BIOSセットアップでUSBを使用できるように設定する必要があります。
  BIOS セットアップについては、パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」を参照してください。

■コンピュータの修理について

コンピュータを修理に出す場合、修理後の設定が修理前とは異なることがあります。そのため、修理に出す前や出した後には次の作業が必要になります。

□ 修理前に必要な作業

鍵のバックアップ

「バックアップについて」（→ P.21）をご覧になり、バックアップを行います。

SMARTACCESS による Windows ログオンを使用しない設定に変更する

必ず SMARTACCESS による Windows ログオンを使用しない設定に変更してください。
SMARTACCESS による Windows ログオンを使用する設定にして修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。
また、パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定し、任意のパスワードに変更してから「SMARTACCESS による Windows ログオン」を使用しない設定にしてください。

重要

- SMARTACCESS による Windows ログオンの設定については、次のマニュアルをご覧ください。
  - ・SMARTACCESS/Premium をお使いの場合
    『SMARTACCESS/Premium リファレンスガイド　機能編』の「Windows ログオン」
  - ・SMARTACCESS/Basic をお使いの場合
    『SMARTACCESS/Basic リファレンスガイド　機能編』の「Windows ログオン」

BIOS パスワードを解除する

パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧になり、設定したパスワードを解除してください。

□ 修理後に必要な作業

リストアする

「リストアについて」（→ P.21）の処理に従って、鍵を復元してください。

BIOS パスワードを設定する

パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧になり、パスワードを設定してください。

SMARTACCESS による Windows ログオンを使用する設定に変更する

SMARTACCESS による Windows ログオンを使用していた場合は、『SMARTACCESS/Premium リファレンスガイド　機能編』、または『SMARTACCESS/Basic リファレンスガイド　機能編』の「Windows ログオン」をご覧になり、SMARTACCESS による Windows ログオンを使用する設定に変更してください。
なお、SMARTACCESS による Windows ログオンの設定を変更する前に、「現在の機器構成情報の登録」を行う必要があります。

■コンピュータの廃却について

コンピュータを廃却する前に安全のため、次の手順に従ってセキュリティチップの鍵や、鍵に関連するファイルを削除してください。

重要

- セキュリティチップの鍵や、鍵に関連するファイルを削除すると、セキュリティチップにより保護されていた暗号化ファイルや証明書は利用できなくなります。
- セキュリティチップの鍵を削除すると、セキュリティチップで暗号化したファイルや証明書が利用できなくなります。
  削除する前に、必要に応じて暗号化を解除してください。

1 **「セキュリティチップの鍵を消去するには」（→ P.25）をご覧になり、セキュリティチップの鍵を消去します。**

2 **パソコン本体の『製品ガイド』の「セキュリティ」－「パソコン本体廃棄時のセキュリティ」をご覧になり、ハードディスク内のデータを削除します。**

使い方

重要

- セキュリティチップの設定の変更方法については、次のマニュアルをよくお読みになり、手順に従って設定してください。
  - SMARTACCESS/Premium をお使いの場合
    『SMARTACCESS/Premium リファレンスガイド　機能編』または『SMARTACCESS/Premium リファレンスガイド　ツール編』
  - SMARTACCESS/Basic をお使いの場合
    『SMARTACCESS/Basic リファレンスガイド　機能編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』

■パスワードを変更するには

セキュリティチップに設定した、所有者パスワードおよびユーザーキーパスワードは変更することができます。また、ユーザーキーパスワードは各ユーザで定期的に変更することをお勧めします。
所有者パスワードの変更については、『SMARTACCESS/Premium リファレンスガイド　ツール編』、または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「管理者ツール」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。
ユーザーキーパスワードの変更については、『SMARTACCESS/Premium リファレンスガイド　ツール編』、または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「利用者ツール」－「ユーザー情報管理」－「セキュリティチップ」、「管理者ツール」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。

■パスワードを忘れた場合には

ユーザーキーパスワードを忘れた場合は、再設定することができます。
ユーザーキーパスワードを再設定する場合には、所有者が事前にパスワードリセットの設定を行う必要があります。
パスワードをリセットする場合は、『SMARTACCESS/Premium リファレンスガイド　ツール編』、または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「管理者ツール」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。

■セキュリティチップの鍵を消去するには

コンピュータを廃却する場合には、パソコンに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップ内のデータを破棄し、復元用ファイルを破棄することで再び復元することができなくなります。
セキュリティチップ内のデータを消去する手順については、パソコン本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧ください。

重要

- この操作ではセキュリティチップのデータを破棄するだけで、ハードディスクのデータは破棄されません。
- セキュリティチップのデータを破棄したことで、ハードディスク内のセキュリティチップで保護されたデータは見ることができなくなりますが、実際の廃却時にはハードディスクのデータをクリアしてください。
- BIOS セットアップで、セキュリティチップ関連の設定を行うには、管理者用パスワードを設定する必要があります（FMV-W シリーズ以外の場合）。

■新しいユーザを登録するには

Windows に新規ユーザを追加する場合、そのユーザがセキュリティチップを利用するためには、セキュリティチップに新規ユーザの情報を登録する必要があります。SMARTACCESS では Windows へ新規ユーザを追加し、セキュリティチップの登録を行うことができます。

2 指紋センサー

特長

■コンパクト

弱電界式半導体指紋センサーを採用し、小型の設計になっています。

■照合精度

富士通独自の「適応型特徴相関法[注]」により、高い識別率を可能にしました。富士通独自のアルゴリズムにより、照合も高速で行うことができます。また、登録した指紋の画像は一切残らないため、プライバシー保護の面からも安心してお使いになれます。

注：指紋の模様に含まれる「端点」や「分岐点」などの特徴点の相対的なつながりを利用して識別精度を飛躍的に高くする方法です。通常、特徴点だけでも十分な認識精度が得られるのに加え、特徴点相互間の相関を計算することで識別能力が高くなると同時に、指紋の歪みや汗に影響を受けずに認識できる利点があります。

使用上のご注意

■指紋センサー使用時のご注意

センサー部に強い衝撃を与えないでください。故障の原因となることがあります。

■指紋登録時／照合時のご注意

・指の状態が次のような場合には、指紋の登録が困難になったり、照合率が低下することがあります。
  - 汗や脂が多い
  - 手が荒れたり、極端に乾燥している
  - 指に傷がある、または磨耗して指紋が薄い
  - 急に太ったり、やせたりして指紋が変化した

  手を洗う、手を拭く、登録する指を変えるなどお客様の指の状態に合わせて対処することで、登録時や照合時の状況が改善されることがあります。
・指紋の登録や照合を行う場合、センサー上で指を正しくスライドさせてください（→P.28）。スライドのさせ方が正しくないと、指紋の中心がセンサー中央からずれて、指紋を読み取ることが困難になったり、照合率が低下することがあります。

■センサーに関するご注意

・指紋の読み取りを行う前に金属に手を触れるなどして、静電気を取り除いてください。静電気が故障の原因となる場合があります。冬季など乾燥する時期は特にご注意ください。
・センサー部分をひっかいたり、先のとがったもので押したりしないでください。傷がつく原因となります。
・使用中はセンサー表面が温かくなることがありますが、故障ではありません。

■センサー表面の清掃について

・次のような場合は指紋の読み取りが困難になったり、照合率が低下することがあります。センサー表面はときどき清掃してください。
  - センサー表面がほこりや皮脂などで汚れている
  - センサー表面に汗などの水分が付着している
  - センサー表面が結露している
・次のような現象が起きる場合は、センサー表面を清掃してください。現象が改善されることがあります。
  - 指を置いていないのに「初期化中に画像を検出しました」というエラーが表示される
  - 指を離しているのに「指を離してください」の表示が出たままになる
  - 認証画面から「バイオパスワード認証」ウィンドウに切り替えられない
  - 指紋の登録失敗や照合失敗が頻発する
・清掃の際には、乾いたやわらかい布でセンサー表面の汚れを軽く拭き取ってください。

重要

▶ **センサー表面に水などの液体をたらさないでください。また、ベンジンなどの揮発性有機溶剤や化学ぞうきんは使用しないでください。**

■その他のご注意

・指紋認識技術は完全な本人認識・照合を保証するものではありません。当社では指紋センサーを使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切責任を負いかねますのであらかじめご了承ください。
・指紋センサーは、パソコン用機器として設計されております。人命に関わる用途、または高度な信頼性、安全性を要する用途での使用は考慮されておりません。このような用途で使用される設備、機器、システム等への組み込みは避けてください。
・指紋センサーは、日本国内仕様であり、添付のアプリケーション、ドライバなどは各 OS の日本語版のみ対応しております。

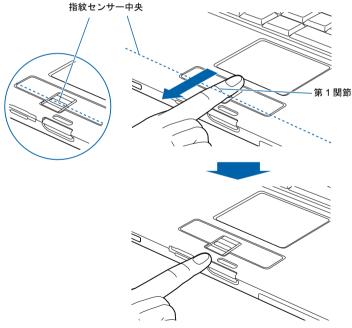
使い方

■指紋を読み取る

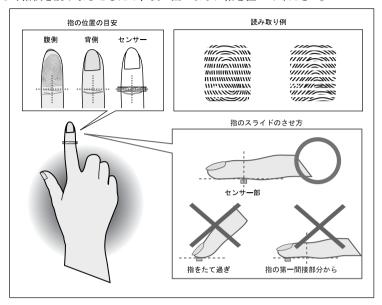
指紋の登録や認証を行う場合は、次のように指をスライドさせてください。認証の失敗を減らすことができます。

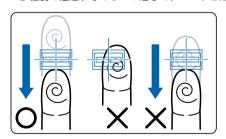
1 操作する指の第一関節が、指紋センサーの中央部に当たるように準備します。

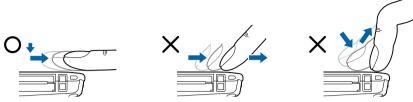
第一関節より先の部分が読み取り範囲となります。

2 第一関節を指紋センサーに押し当てると同時に指を動かし、センサー部が完全に見えるまで水平にスライドします。

（イラストは機種や状況により異なります）

□ 指のスライドのさせ方について

正しく指紋を読み取らせるため、次の図のように指を置いてください。

重要

- うまく認識されないときは
  次の点に気を付けて操作してください。
  - ・指の第一関節より先の部分が、指紋センサー上を通過するようにする
  - ・指紋の渦の中心が、指紋センサーの中心を通過するようにする
  - ・1 秒程度で通過するくらいの速さで、スーッと動かす

  なお、親指など、指紋の渦の中心を合わせにくい指は、うまく認識できないことがあります。その際は、中心を通過させやすい指を登録してください。
- 指紋の読み取りがうまくいかない場合
  指のスライドが速すぎたり遅すぎたりした場合、正常に認識できないことがあります。画面のメッセージに従って、スライドの速さを調節してください。

- 指を突き立てたり、引っかけるようにスライドさせないでください。
  指紋センサーに指のはら（指紋の中心部）が接触していなかったり、指を引っかけるようにスライドさせると指紋の読み取りがうまくいかない場合があります。
  必ず、指のはら（指紋の中心部）が指紋センサーに接触するようにスライドさせてください。

（イラストは機種や状況により異なります）

- 指紋の読み取りがうまくいかない場合
  指のスライドが速すぎたり遅すぎたりした場合、正常に認識できないことがあります。画面のメッセージに従って、スライドの速さを調節してください。

■指紋センサーのスクロール機能を使用する

指紋センサードライバをインストールすると、指紋センサーのスクロール機能で、画面のスクロールをすることができるようになります。ウィンドウ内のスクロールする領域をクリックしてから、指紋センサー上で指先を前後方向にスライドすると、指の動きに合わせてウィンドウ内の表示が上下にスクロールします。

POINT

- 対象とするウィンドウによっては、スクロール機能が使用できない場合があります。
- スクロールの速度については、「コントロールパネル」の「指紋センサー」から調整することができます。「指紋センサー」が表示されていない場合は、ウィンドウ左側の「コントロールパネルのその他のオプション」をクリックしてください。

3 FeliCa 対応リーダ／ライタ

FeliCa は、ソニー株式会社が開発した非接触 IC カードの技術方式です。コンピュータに内蔵の FeliCa 対応リーダ／ライタを利用して、コンピュータのセキュリティを向上するための環境を提供します。

使用上のご注意

■FeliCa 対応非接触 IC カードについて

FeliCa 対応非接触 IC カードは添付されていません。弊社純正品「FeliCa 対応非接触 IC カード（SMARTACCESS 専用）（FMFLC-C1）」を別途ご購入ください。
なお、FeliCa 対応非接触 IC カードは SMARTACCESS 専用のカードです。SMARTACCESS 以外のソフトウェアや、入退室管理システムなどのサービスにはご使用できません。また、FeliCa 対応非接触 IC カードに、他のソフトウェアやサービスを追加フォーマットすることはできません。

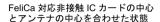
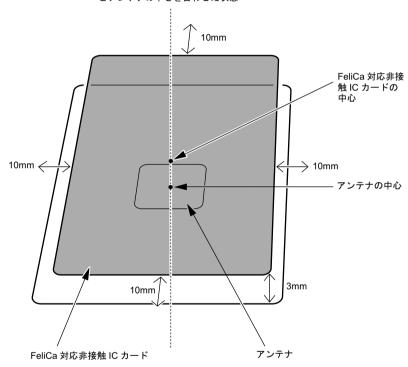
■FeliCa 対応リーダ／ライタ利用についてのご注意

- FeliCa 対応リーダ／ライタで使用するソフトウェアをインストールするときには、コンピュータ本体またはネットワーク上のコンピュータに、CD/DVD ドライブが搭載、または接続されている必要があります。
- 外付けの FeliCa 対応リーダ／ライタ（PaSoRi）を同時に使うことはできません。また、外付けの FeliCa 対応リーダ／ライタ（PaSoRi）はサポートしておりません。
- コンピュータ本体の修理や保守を依頼する場合は、SMARTACCESS/PremiumのWindowsログオン機能を解除してください。また、パスワードの自動生成を行っている場合は、一度自動生成を解除した後「パスワードの変更」より任意のパスワードに変更してからWindowsログオン機能の解除を行ってください。
  Windowsログオン機能を解除していない場合、修理や保守ができないことがあります。
  Windowsログオン機能を解除するには、SMARTACCESS/Premiumの環境設定を使用して設定を変更する必要があります。
  環境設定は、FeliCa対応リーダ／ライタを搭載するコンピュータやそれを含むシステムを管理する方のみお使いになれます。詳しくは、『SMARTACCESS/Premiumリファレンスガイド　機能編』または『SMARTACCESS/Premiumリファレンスガイド　ツール編』をご覧ください。
- コンピュータ本体の修理や保守が行われた場合には、セキュリティ機能が解除されていることがあります。その場合は環境の再構築が必要となります。『SMARTACCESS/Premium リファレンスガイド　機能編』または『SMARTACCESS/Premium リファレンスガイド　ツール編』をご覧になり、再設定を行ってください。
- コンピュータ本体で、リカバリを実行した場合、FeliCa 対応リーダ／ライタで使用するソフトウェアは再度インストールする必要があります。

使い方

コンピュータ本体に内蔵されているFeliCa対応リーダ／ライタは､鉄道の改札機などのリーダ／ライタと比べると電波強度が弱いため、FeliCa 対応非接触 IC カードを認識できる範囲が限られます。良好な通信が保証される範囲の目安は、次のとおりです（カードの種類によって若干異なります)。

・アンテナ表面からの距離は、3mm 以下

・FeliCa 対応非接触 IC カードの中心とアンテナの中心を合わせた状態から、前後左右に 10mm 以内

（イラストは機種により異なります）

重要

▶ お使いの機種によりアンテナの位置が異なります。アンテナの位置については、パソコン本体の『製品ガイド』の「各部名称」を参照してください。

4 スマートカードリーダ／ライタ

スマートカードによる BIOS ロックの設定

スマートカードによる BIOS ロック機能をお使いになるには、コンピュータ本体の BIOS 設定を変更する必要があります。次の注意を参照し、正しく設定してください。
BIOS 設定の変更方法については、パソコン本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧ください。

重要

- スマートカードのPIN入力を連続して15回間違えて入力するとカードがロックされ使用できなくなります。
  ロックされたスマートカードではコンピュータにログオンできなくなるので PIN は忘れないようにしてください。
- BIOSの設定を変更する前に、スマートカードにBIOSロック用パスワードを登録してください。登録方法については、『SMARTACCESS/Premiumリファレンスガイド　ツール編』または『SMARTACCESS/Basicリファレンスガイド　ツール編』の「利用者ツール」－「ログオン情報の登録」－「BIOSパスワード」をご覧ください。
- BIOS ロック用パスワードを登録せずに本設定を行うと、コンピュータが起動できなくなります。
- BIOS ロック用パスワードでお使いになれる文字は、半角英数字（a ～ z, A ～ Z, 0 ～ 9）のみで、大文字・小文字が区別されます。
- 半角英数字以外の文字をお使いになると、コンピュータが起動できなくなります。
- ユーザー用パスワード設定は、管理者用パスワード設定がされていないと行えません。
- BIOS でロックをかけるときには、1 枚のカードに 1 つのパスワードしか設定できません。
- BIOS でロックをかけるスマートカードは、利用者が『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』に従って作成してください。また、複数のスマートカードをお使いになる場合、管理者用スマートカードを作成してから、ユーザー用スマートカードを作成してください。

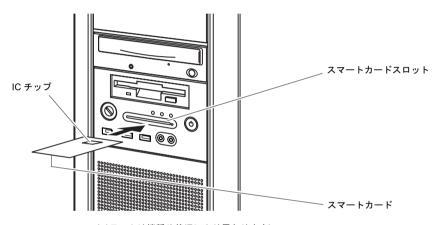
使用上のご注意

- 他の装置で作成した、拡張情報の多いスマートカードの読み取りをスマートカードリーダ／ライタで行うと、ごくまれにスマートカードの機能が停止する場合があります。
  このような場合、コンピュータを再起動してください。再起動後、スマートカードリーダ／ライタで作成したスマートカードをお使いになるか、拡張情報を減らした形式で作成し直したスマートカードをお使いください。
- スマートカードは IC チップ面を上にして、奥までゆっくり差し込んでください。
- Windows を再起動する場合は、「OK」または「はい」をクリックして再起動を実行してから、起動画面が出るまでの間に、スマートカードを抜いてください。
- Windows を正常にシャットダウンした場合およびスタンバイ状態のときにスマートカードを挿入すると、コンピュータは電源が入ったりレジュームしたりします。

使い方

スマートカードは IC チップ面を上にして、奥までゆっくり差し込みます（スマートカードスロットの位置などについてはパソコンまたはワークステーション本体の『製品ガイド』をご覧ください）。

POINT

- スマートカードリーダ／ライタにスマートカードを差し込むことによりコンピュータの電源を入れたり、スタンバイ状態からレジュームさせることができます。
  ただし、コンピュータの設定や、電源を切った状態によっては、電源が入らない場合があります。詳しくは、「使用上のご注意」（→ P.33）をご覧ください。

（イラストは機種や状況により異なります）

重要

- スマートカードを使用するときは、次の点に注意してください。
  - 折り曲げたり、汚したり、濡らしたりしないでください。
  - 磁石などの磁気を帯びたものを近づけないでください。
  - 電気を帯びたものを上に載せたり、近くで静電気を発生させたりしないでください。
  - 高温の場所に保管しないでください。
  - カードに衝撃を与えないでください。
- スマートカードをご購入の際は、「富士通パーソナル製品に関するお問合せ窓口」、またはご購入元にご連絡ください。

5 スマートカードホルダー

スマートカードによる BIOS ロックの設定

スマートカードによる BIOS ロック機能をお使いになるには、パソコン本体の BIOS 設定を変更する必要があります。次の注意を参照し、正しく設定してください。
BIOS 設定の変更方法については、パソコン本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧ください。

重要

- スマートカードのPIN入力を連続して15回間違えて入力するとカードがロックされ使用できなくなります。
  ロックされたスマートカードではコンピュータにログオンできなくなるので PIN は忘れないようにしてください。
- BIOSの設定を変更する前に、スマートカードにBIOSロック用パスワードを登録してください。
  登録方法については、『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basicリファレンスガイド　ツール編』の「利用者ツール」－「ログオン情報の登録」－「BIOSパスワード」をご覧ください。
- BIOS ロック用パスワードを登録せずに本設定を行うと、コンピュータが起動できなくなります。
- BIOS ロック用パスワードでお使いになれる文字は、半角英数字（a ～ z, A ～ Z, 0 ～ 9）のみで、大文字・小文字が区別されます。
- 半角英数字以外の文字をお使いになると、コンピュータが起動できなくなります。
- ユーザー用パスワード設定は、管理者用パスワード設定がされていないと行えません。
- BIOS でロックをかけるときには、1 枚のカードに 1 つのパスワードしか設定できません。
- BIOS でロックをかけるスマートカードは、利用者が『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』に従って作成してください。また、複数のスマートカードをお使いになる場合、管理者用スマートカードを作成してから、ユーザー用スマートカードを作成してください。

使用上のご注意

- BIOS の設定を変更する前に、スマートカードに BIOS ロック用パスワードを登録してください。
  登録方法については、『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「利用者ツール」－「ログオン情報の登録」－「BIOS パスワード」をご覧ください。
  BIOS ロック用パスワードを登録せずに本設定を行うと、コンピュータが起動できなくなります。
- BIOS ロック用パスワードで使用できる文字は、半角英数字（a ～ z，A ～ Z，0 ～ 9）のみです。なお、スマートカードには大文字と小文字が区別して記録されますが、BIOS では大文字と小文字は区別されません。
  半角英数字以外の文字をお使いになると、コンピュータが起動できなくなります。

- BIOS ロック用パスワードは、1 枚のカードに 1 つのパスワードしか設定できません。
  BIOS でロックをかけるスマートカードは、利用者が『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』に従って作成してください。また、複数のスマートカードをお使いになる場合、管理者用スマートカードを作成してから、ユーザー用スマートカードを作成してください。
- スマートカードホルダーをセットしていない場合は、BIOS セットアップに「スマートカードによるロック」の項目は表示されません。
- 「SMARTACCESS」で管理者PIN（Personal Identification Number）および利用者PINを変更する場合は、1～16桁の半角英数字を使用してください。

■設定方法

□ スマートカードの作成

『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』をご覧になり、管理者用およびユーザー用スマートカードを作成します。スマートカードの作成は、管理者用を作成したあと、ユーザー用を作成してください。

□ コンピュータ側の設定

コンピュータに、スマートカードを作成したときに登録したパスワードを登録します。

重要

▶ BIOS セットアップについては、パソコン本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧ください。

■スマートカード利用についてのご注意

- スマートカードホルダーは、IC チップを使用した大変デリケートな電子部品です。
  パソコン本体への取り付け／取り外しを行う場合には、落下などの衝撃を与えないでください。
- 寿命について
  スマートカードは、カードに搭載されている IC チップを、ホルダー内部のソケットに接触させることによって、IC チップに内蔵されている情報の読み取り／書き込みを行います。そのため、同じカードホルダーを長期間にわたって使用していると、IC チップ・ソケットなどの電子部品が消耗して、正しい情報の読み取り／書き込みができなくなってきます。保守作業として定期的にカード・ホルダーを交換することをお勧めします。
  なお、次の状態になった場合を交換の目安としてください。
  - スマートカードを挿入してもカードが認識されなくなってきた場合
  - カードが読み取りにくくなってきた場合
  - データの更新に時間がかかるようになってきた場合
- スマートカードホルダーで使用するアプリケーションのインストール時には、コンピュータ本体またはネットワーク上のコンピュータに、CD ドライブが搭載／接続されている必要があります。
- スマートカードが動作している場合、アクセスに数分程度時間がかかる場合があります。
- スマートカードは IC チップ面を上にして、奥までゆっくり差し込んでください。
- コンピュータを持ち運ぶ場合は、スマートカードを取り出しておいてください。
- スマートカードホルダーを PC カードスロットにセット／取り出す場合は、スマートカードをスマートカードホルダーから取り出しておいてください。

・スマートカードホルダーは、1 台のパソコン本体に 1 つのみセットできます。同時に 2 つ以上をセットしないでください。
・コンピュータの修理・保守を依頼される場合は、BIOS ロック用パスワードを解除しておいてください。BIOS ロック用パスワードが解除されていない場合は、修理・保守などができない場合があります。
・他の装置で作成した、拡張情報の多いスマートカードの読み取りをスマートカードホルダーで行うと、ごくまれにスマートカードの機能が停止する場合があります。
このような場合、コンピュータを再起動してください。再起動後、スマートカードホルダーで作成したスマートカードをお使いになるか、拡張情報を減らした形式で作成し直したスマートカードをお使いください。
・スマートカードホルダーは、他のスマートカードリーダ装置と同時に使用することはできません。
・スタンバイや休止状態からレジューム（復帰）後、もう一度スタンバイや休止状態を行う場合は、しばらく（30 秒程度）待ってから操作してください。

使い方

スマートカードホルダーは、コンピュータの PC カードスロットにセットします。PC カードスロットの位置や使い方については、パソコン本体の『製品ガイド』をご覧ください。
スマートカードは IC チップ面を上にして、奥までゆっくり差し込みます。

（イラストは機種や状況により異なります）

第 3 章

SMARTACCESS の機能概要

SMARTACCESS には、不正アクセスや情報漏えいへの対策として、複数の認証デバイスを使ったログオン認証、不正デバイスの使用防止などの機能があります。
この章では、SMARTACCESS の主な機能について説明しています。

1 セキュリティ対策

使用する権限のない人に不正にコンピュータを使われて、データが破壊されたり漏えいしたりする危険からコンピュータを守ることが必要になってきています。SMARTACCESS では不正使用対策や情報漏えい対策として、指紋センサーによる本人認証や、セキュリティチップによるデータ保護、カードによるログオン情報の保護ができます。複数の認証デバイスを組み合わせることによって、コンピュータの安全性も高まります。

不正使用対策

■ Windows ログオン

悪意のある第三者によって不正に Windows にログオンされることを防ぎます。
Windows の起動時やコンピュータのロック、休止状態からの復帰、スクリーンセーバーからの復帰時に入力するユーザー名、パスワードを認証デバイスに設定できます。複数の認証デバイスを組み合わせて使用すればパスワードを入力するだけの認証よりもさらにセキュリティが高まります。

■ アプリケーションログオン

ユーザー名／パスワードで運用している Web やアプリケーションなどのセキュリティレベルを強化します。
パスワード認証を必要とするアプリケーションやWebサイトをあらかじめ登録しておくと、暗号化して認証デバイスに格納されているユーザー名やパスワードを利用してアプリケーションにログオンします。
認証デバイスにパスワードを格納しておくことによって、パスワードを入力するだけの認証よりもさらにセキュリティが高まります。

情報漏えい対策

■ Windows 暗号化ファイルシステム（EFS）の鍵をセキュリティチップで保護

ハードディスクに保存されているファイルをより強固に守ります。
Windows でファイルとフォルダの暗号化を設定することにより、暗号化に利用される鍵をセキュリティチップで安全に管理します。
ハードディスクを盗まれた場合にも暗号鍵を解析され、暗号化した機密文書が漏えいしてしまうことがありません。

■機器監査

あらかじめ機器構成を登録して Windows 起動時に機器監査を行い、第三者によって登録外の機器構成に変更された場合にログオンを拒否できます。これにより使用者の意図しない不正なハードウェアが取り付けられることを防ぎます。
セキュリティチップを搭載したコンピュータでお使いになれます。
詳しくは、「認証デバイスについて」－「セキュリティチップ」－「使用上のご注意」－「機器監査について」（→ P.22）をご覧ください。

■機器制限

USB や光学ドライブ、シリアル、パラレル、赤外線通信などの各ポートの使用を制限して不正なハードウェアが取り付けられることを防ぎます。これによりコンピュータからの重要データの持ち出しを未然に防ぎます。
この機能は Portshutter や FENCE-G と連携することでお使いになれます。

重要

- FENCE-G との連携機能をお使いになるには、SMARTACCESS/Premium が必要です。

2 運用管理機能

SMARTACCESS には、運用管理機能として「利用ログ管理」機能や「バックアップツール」があります。また、SMARTACCESS の運用を統合化するために Systemwalker や Active Director との連携機能があります。

セキュリティイベントの監査

システムで発生したエラーや警告などのログ情報をログファイルに格納します。コンピュータ上で不正アクセスの原因や利用状況などを追跡できます。
また、Systemwalker と連携することができます。これにより、ログオン情報を一元管理して管理画面からリアルタイムに状況を把握することが可能になります。例えば、ログオンを何回も失敗しているユーザーがいるといった異常な状態を、リアルタイムで把握できます。

重要

- この機能をお使いになるには、SMARTACCESS/Premium が必要です。

障害からの復旧

ファイル装置や認証デバイスなどの障害による、SMARTACCESS の環境設定情報やユーザー情報の損失に備え、バックアップファイルを作成します。また、障害により環境設定情報やユーザー情報を損失した場合は、バックアップファイルから復元できます。

ネットワーク管理

企業規模がある程度以上になると、全社規模でのコンピュータのセキュリティ管理が重要になってきます。それぞれのコンピュータで管理していた認証用の情報や SMARTACCESS の利用環境の情報をネットワークレベルで集中管理することができます。
バイオ認証装置と連携することで、指紋などの認証用の情報をバイオ認証装置で一元管理でき、さらにバイオ認証を行うことができます。
また、Windows ドメイン環境では、Active Directory と連携した運用ができます。SMARTACCESS の利用環境をドメインレベルで管理でき、利用環境の標準化が維持できます。

重要

- この機能をお使いになるには、SMARTACCESS/Premium が必要です。

3 認証デバイスと SMARTACCESS で実現する機能

セキュリティチップ

セキュリティチップは内部に暗号鍵を保持し、Windows ログオンやアプリケーションログオンで使用するパスワードなどを暗号化するセキュリティ専用のハードウェアです。セキュリティチップで管理された暗号鍵は外部に出す方法がないので、データが万一外部に持ち出されたとしてもデータの内容を復号化することはできません。
また、ユーザーごとに鍵を生成することができるので、データを安全に管理することができます。

■暗号鍵の保護

・Windows 暗号化ファイルシステム（EFS）用の暗号鍵をセキュリティチップで管理
・セキュリティチップによる PKI 暗号処理および暗号鍵の管理

■パスワードの保護

・Windows やアプリケーションや Web サイトの ID、パスワードをセキュリティチップで暗号化
・あらかじめ登録したアプリケーションや Web サイトのパスワード入力画面が表示されたときの自動入力機能

■機器監査

Windows 起動時に BIOS の構成情報などを監査し、不正な機器の取り付けなど、機器の構成が変更されていると、警告を表示するか、または Windows ログオンを拒否します。
これにより使用者の意図しない不正なハードウェアが取り付けられることを防ぎます。
詳しくは、「認証デバイスについて」－「セキュリティチップ」－「使用上のご注意」－「機器監査について」（→ P.22）をご覧ください。

■ユーザーキーパスワード

SMARTACCESS でセキュリティチップを使って Windows やアプリケーションにログオンする場合は、セキュリティチップに対するパスワード（ユーザーキーパスワード）を使用します。
ユーザーキーパスワードは通常の Windows パスワードよりも長い文字列を扱うことができるためセキュリティを高めることができます。
ユーザーキーパスワードを入力すると、セキュリティチップによって暗号化されたユーザー名やパスワードを復号化できます。ユーザーキーパスワードを 1 つだけ覚えれば、複雑なパスワードをアプリケーションごとに覚える必要はありません。

指紋センサー

人により異なる特徴を持つ「指紋」を利用した認証ができます。また、指を置くだけの簡単な操作で本人認証ができ、他人にパスワードを盗み見られる心配がありません。

■ パスワードの保護

Windows やアプリケーションや Web サイトのユーザー名やパスワードを手入力する代わりに指紋で本人認証を行うことにより安全性が高まります。

IC カード（FeliCa 方式）

非接触 IC カード技術方式「FeliCa」に対応した IC カードに、ユーザー名やパスワードなどのセキュリティ情報を格納します。このカードを、FeliCa 対応リーダ／ライタにタッチまたはセットすることで、コンピュータ本体にセキュリティ情報を認識させます。IC カード（FeliCa 方式）を持ち運ぶことにより、不正利用を防止します。

重要

- IC カード（FeliCa 方式）をお使いになるには、SMARTACCESS/Premium が必要です。

■ パスワードの保護

- Windows やアプリケーション、Web サイトの ID、パスワードを IC カード（FeliCa 方式）に格納します。
- あらかじめ登録したアプリケーションや Web サイトのパスワード入力画面が表示されたときの自動入力機能があります。

■ IC カード（FeliCa 方式）監視

IC カード（FeliCa 方式）抜き取りまたはタッチ時にコンピュータをロックします。
離席時にカードを操作することにより、コンピュータを自動的にロックし、不正利用を防ぐ機能です。

■ カード管理リスト

IC カード（FeliCa 方式）の属性を集中管理します。
IC カード（FeliCa 方式）紛失時などに、IC カード（FeliCa 方式）の無効化設定を行い、不正利用を防ぐ機能です。

スマートカード

接触型スマートカードに、ユーザー名やパスワード、証明書などのセキュリティ情報を格納します。このスマートカードをリーダ／ライタに挿すことで、コンピュータ本体にセキュリティ情報を認識させます。スマートカードを持ち運ぶことにより、不正利用を防止します。

■パスワードの保護

・Windows やアプリケーション、Web サイトの ID、パスワードをスマートカードに格納します。
・あらかじめ登録したアプリケーションや Web サイトのパスワード入力画面が表示されたときの自動入力機能があります。

■スマートカードの抜き取り監視

スマートカード抜き取り時にコンピュータをロックします。
離席時にスマートカードを抜くことにより、コンピュータを自動的にロックし、不正利用を防ぐ機能です。

第 4 章

インストールと設定

各認証デバイスを使ったセキュリティ対策機能などをお使いになるには、認証デバイスおよび SMARTACCESS のインストール、利用するセキュリティ環境にあったセットアップが必要です。
この章では、認証デバイスや SMARTACCESS の導入からお使いになるまでの基本的な流れを説明しています。

1 導入モデル

SMARTACCESS は、スタンドアロンまたはワークグループ環境、ドメイン環境で、認証デバイスを利用するセキュリティ環境を構築できます。また、セキュリティ環境を構築する側、セキュリティ環境を利用する側、それぞれでSMARTACCESS の使用権限が異なります。

SMARTACCESS での管理者と利用者

SMARTACCESS を使ったセキュリティ環境を構築する側を「管理者」、そのセキュリティ環境を利用する側を「利用者」と呼びます。
管理者は最適なセキュリティ環境を利用者に提供するための設定および管理を行い、利用者はそのセキュリティ環境により認証デバイスを利用して安全にコンピュータにアクセスすることができます。

SMARTACCESS には、セキュリティ環境を構築するツールとして「環境設定」、利用者固有の情報を管理するツールとして「ユーザー情報設定」があります。
管理者および利用者の権限と主な実行可能ツールは次のとおりです。

	スタンドアロンまたはワークグループ環境	ドメイン環境	実行可能ツール
管理者	ローカルコンピュータのAdministratorsグループのメンバー	ActiveDirectory（ドメインコントローラ）のDomain Admins グループのメンバー	環境設定／ユーザー情報設定
利用者	Usersグループのメンバー	Domain Usersグループのメンバー	ユーザー情報設定

運用形態

SMARTACCESS の主な運用形態は次のとおりです。

■1 台のコンピュータで管理者と利用者が同一の運用

導入から環境の設定、利用するまでを一括して一人で行います。主に個人ユーザーが利用する場合の運用形態です。

■1 台のコンピュータで管理者と利用者が異なる運用

導入から環境の設定まで、一連の構築を管理者が行います。利用者は管理者が構築した環境で SMARTACCESS を利用します。

■1 台のコンピュータを複数の利用者が使う運用

複数の利用者が 1 台のコンピュータを共有して使う場合、導入から利用者ごとの環境の設定までを管理者が行います。利用者は利用者ごとに設定された環境で SMARTACCESS を利用します。

■ネットワーク運用

バイオ認証装置やActiveDirectoryと連携し、1台のコンピュータが認証用の情報やSMARTACCESSの環境設定情報を一括して管理します。利用者はスタンドアロンまたはワークグループ環境と同等にお使いになれます。
ネットワーク運用については、「ネットワーク運用」（→ P.107）をご覧ください。

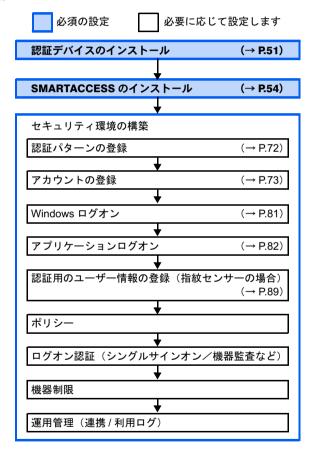
重要

- バイオ認証装置や Active Directory との連携機能をお使いになるには、SMARTACCESS/Premium が必要です。

2 作業の流れ

導入の手順は、お使いになる認証デバイスやセキュリティ環境によって異なります。主な手順は次のとおりです。

□ 用意するもの

・パソコンまたはワークステーション本体
・ドライバーズディスク（SMARTACCESS/Basic の場合）、または「SMARTACCESS/Premium」CD-ROM

POINT

▶ この章では、例として指紋認証による「Windows ログオン」と「アプリケーションログオン」の基本的なセキュリティ構築の流れを説明しています。

3 認証デバイスのインストール

SMARTACCESS をインストールする前に、お使いになる認証デバイスのインストールが必要です。SMARTACCESS では、複数の認証デバイスを組み合わせて利用することもできます。

BIOS の設定を変更または確認する

次の認証デバイスをお使いになる場合、認証デバイスをインストールする前に必ず BIOS の設定を変更または確認してください。

- セキュリティチップ
- FeliCa 対応リーダ／ライタ

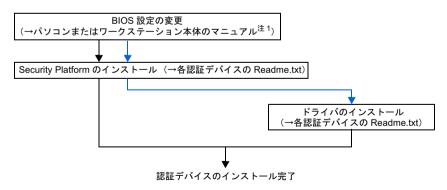
□ セキュリティチップをお使いになる場合

パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧になり、BIOS の設定を変更してください。

□ FeliCa 対応リーダ／ライタをお使いになる場合

パソコン本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧になり、BIOS の設定を確認してください。

認証デバイスのインストール

認証デバイスのインストール手順は次のとおりです。

注 1 : パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」

重要

- 認証デバイスをインストールするときは、管理者権限で Windows にログオンする必要があります。
- 認証デバイスをインストールする前には、使用中のソフトウェアをすべて終了させてください。
- スマートカードをお使いになる場合、ドライバのインストール後に次の手順でスマートカードの設定を確認してください。
  1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
     「コントロールパネル」ウィンドウが表示されます。
  2. 「パフォーマンスとメンテナンス」→「管理ツール」→「サービス」の順にクリックします。
     「サービス」ウィンドウが表示されます。
  3. 「Smart Card」の「スタートアップの種類」が「自動」になっていることを確認します。
     「スタートアップの種類」が「自動」になっていない場合は次の手順に進みます。
     「自動」になっている場合は、確認はこれで完了です。
  4. 「Smart Card」をダブルクリックします。
     「（ローカル コンピュータ）Smart Card のプロパティ」ウィンドウが表示されます。
  5. 「全般」タブの「スタートアップの種類」から「自動」を選択します。
  6. 「OK」をクリックし、すべてのウィンドウを閉じます。

認証デバイスのインストール方法については、次のディスク内に格納されているそれぞれの認証デバイスの「Readme.txt」をご覧ください。

FMV シリーズのカスタムメイドで、FeliCa 対応リーダ／ライタを選択した場合

パソコン本体に添付の「SMARTACCESS/Premium」CD-ROM に格納されています。

セキュリティチップ内蔵の FMV シリーズ、CELSIUS シリーズをご購入の場合

FMV シリーズまたは CELSIUS シリーズのカスタムメイドで、指紋センサー、スマートカードホルダー、またはスマートカードリーダ／ライタを選択した場合

パソコンまたはワークステーション本体に添付の「ドライバーズディスク」に格納されています。

それぞれの認証デバイスの「Readme.txt」が格納されているフォルダは次のとおりです。

□ SMARTACCESS/Premium の場合（「SMARTACCESS/Premium」CD-ROM 内）

認証デバイス		格納先フォルダ
指紋センサー	指紋センサー	¥fingerprint
	指紋認識エンジン	¥FSTDrv
セキュリティチップ		¥IFXSW20
FeliCa 対応リーダ／ライタ		¥SONY FeliCa リーダー _ ライター

注：スマートカードをお使いになる場合、「SMARTACCESS/Premium」CD-ROM にはスマートカード用のドライバが格納されておりません。
お使いのパソコンまたはワークステーションに添付の「ドライバーズディスク」（→ P.53）をご覧ください。

□ SMARTACCESS/Basic の場合（「ドライバーズディスク」内）

<table>
<tr><th colspan="2">認証デバイス</th><th>格納先フォルダ</th></tr>
<tr><td rowspan="2">指紋センサー
（FMV-LIFEBOOK）</td><td>指紋センサー</td><td>¥Other¥fingerprint</td></tr>
<tr><td>指紋認識エンジン</td><td>¥Other¥FSTDrv</td></tr>
<tr><td colspan="2">セキュリティチップ</td><td>¥Other¥IFXSW20</td></tr>
<tr><td colspan="2">スマートカードリーダ／ライタ
（FMV-ESPRIMO、CELSIUS シリーズ）</td><td>¥Other¥Smart</td></tr>
<tr><td colspan="2">スマートカードホルダーまたはスマートカードスロット
（FMV-LIFEBOOK）</td><td>¥Other¥O2scb2kxp</td></tr>
</table>

4 SMARTACCESS のインストール

認証デバイスのインストール完了後、コンピュータが再起動したら、SMARTACCESS をインストールします。

準備

□ SMARTACCESS をインストールする前に

あらかじめ次のことを確認してください。

・SMARTACCESS は Windows ログオン認証を行うソフトウェアと併用することができません。SMARTACCESS をインストールする場合は、必ず他の Windows ログオン認証ソフトウェアをアンインストールしてください。

□ Windows 2000 をお使いの場合

Windows 2000 をお使いの場合、「ユーザー権利の割り当て」の設定を変更する必要があります。SMARTACCESS をインストールするには、Windows アカウントの管理者権限を持つユーザーである必要があります。

1 **「スタート」ボタン→「コントロールパネル」の順にクリックします。**

「コントロールパネル」ウィンドウが表示されます。

2 **「パフォーマンスとメンテナンス」→「管理ツール」→「ローカル セキュリティ ポリシー」の順にダブルクリックします。**

「ローカル セキュリティ設定」が起動します。

3 **ツリーから「ローカル ポリシー」→「ユーザー権利の割り当て」の順にクリックします。**

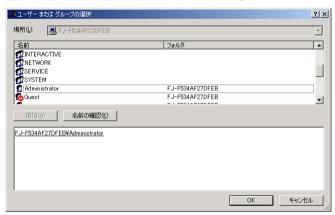
4 **ポリシーから「オペレーティングシステムの一部として機能」をダブルクリックします。**

「ローカル セキュリティ ポリシーの設定」ウィンドウが表示されます。

5 **「追加」をクリックします。**

「ユーザーまたはグループの選択」ウィンドウが表示されます。

6 **名前から管理者権限のユーザーまたはグループを選択して「追加」をクリックします。**

選択した管理者がウィンドウ下側に表示されます。

7 **「OK」をクリックして、「ローカル セキュリティ ポリシーの設定」ウィンドウに戻ります。**

8 **適用先一覧に手順 6 で選択したアカウントが追加されことを確認し、「OK」をクリックします。**

「ローカル セキュリティ設定」ウィンドウに戻ります。

9 **「ファイル」→「終了」の順にクリックします。**

「ローカルセキュリティ設定」が終了します。

10 **コンピュータを再起動して、設定を有効にします。**

重要

- 「ローカルセキュリティ設定」については、Windows2000 のヘルプをご覧ください。

SMARTACCESS のインストール

□ インストールの権限について

SMARTACCESSをインストールするには、Windowsアカウントの管理者権限を持つユーザーである必要があります。
運用形態とインストールする管理者権限の関係は、次のとおりです。

運用形態	必要とする権限
スタンドアロンまたはワークグループ環境	ローカルコンピュータの Administrators グループのメンバー
ドメイン環境	ActiveDirectory（ドメインコントローラ）の Domain Admins グループのメンバー

□ SMARTACCESS のインストール

SMARTACCESS のインストールは、インストーラを実行して画面の指示に従いながら行います。
次の手順でインストールを行ってください。

重要

- お使いになる認証デバイスのインストールが完了してから、SMARTACCESS をインストールしてください。SMARTACCESS をインストールした後に認証デバイスをインストールすると、認証デバイスが正常に認識されない場合があります。
- スマートカードをお使いになる場合、スマートカードホルダーを取り付けた状態で SMARTACCESS をインストールする必要があります。
- SMARTACCESS をインストールする前に、使用中のソフトウェアはすべて終了させてください。
- ハードディスクに十分な空き容量（→ P.12）があることを確認してください。

1 **次のディスクをセットします。**

- SMARTACCESS/Premium の場合
  「SMARTACCESS/Premium」CD-ROM
- SMARTACCESS/Basic の場合
  パソコンまたはワークステーション本体に添付の「ドライバーズディスク」

2 **「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。**

3 「名前」に次のように入力し、「OK」をクリックします。

・SMARTACCESS/Premium の場合
　　[CD/DVD ドライブ]:¥SAPremium¥Setup¥setup.exe
・SMARTACCESS/Basic の場合
　　[CD/DVD ドライブ]:¥Other¥SABasic¥Setup¥setup.exe

「SMARTACCESS 用の InstallShield ウィザードへようこそ」と表示されます。

4 「次へ」をクリックします。

「インストール先のフォルダ」が表示されます。

5 インストール先を確認し、「次へ」をクリックします。

インストール先を変更する場合は、「変更」をクリックします。

■ セキュリティチップがインストールされている場合

「セキュリティチップの自動バックアップ保存先設定」ウィンドウが表示されます。

手順 6 に進んでください。

■ セキュリティチップがインストールされていない場合

「プログラムをインストールできる準備ができました」と表示されます。

手順 9 に進んでください。

POINT

- セキュリティチップをお使いになる場合、システムフォルダのあるドライブと、SMARTACCESS のインストール先ドライブは同じ場所にしてください。セキュリティチップが正常に使用できなくなる場合があります。

6 「参照」をクリックして、自動バックアップの保存先を指定します。

「セキュリティチップの緊急時復元設定」ウィンドウが表示されます。

7 「参照」をクリックして、復元用トークンの保存先を指定します。

8 「パスワード」と「パスワードの確認」に、復元用トークンに設定するパスワードを 6 文字以上 256 文字以下で入力します。

「プログラムがインストールできる準備ができました」と表示されます。

9 「インストール」をクリックして、インストールを開始します。

「SMARTACCESS をインストールしています」と表示されます。

インストールが正常に完了すると、「InstallShield ウィザードを完了しました」と表示されます。

10 「完了」をクリックします。

「SMARTACCESS の InstallShield 情報」メッセージが表示されます。

重要

- インストールの完了後に、「コマンドプロンプト」ウィンドウが表示されることがあります。「コマンドプロンプト」ウィンドウは自動的に閉じますので手動で終了しないでください。

11 「はい」をクリックして、コンピュータを再起動します。

SMARTACCESS のインストール情報を有効にするには、Windows の再起動が必要です。

重要

▶ セキュリティチップをお使いになる場合、SMARTACCESS インストール後に「最近使ったファイル」の一覧に、自動バックアップの保存先で指定したファイルと復元用トークンの保存先で指定したファイルが追加されることがありますが、選択しないでください。

□ アップグレード

・SMARTACCESS/PremiumV1.0L10、SMARTACCESS/BasicV1.1L10、SMARTACCESS/BasicV1.0L10からSMARTACCESS/PremiumV1.1L10にアップグレードする場合、SMARTACCESSのインストールと同じ手順で行うことができます。インストールを実行すると、既存のSMARTACCESSの設定を維持したままでアップグレードができます。
・アップグレードは、旧バージョンをインストールした管理者権限を持つユーザーでログオンしている必要があります。

重要

▶ アップグレードの際の不測の事故に備え、アップグレードを行う前に旧バージョンのバックアップを行ってください。バックアップについては、『SMARTACCESS/Premiumリファレンスガイド　ツール編』または『SMARTACCESS/Basicリファレンスガイド　ツール編』をご覧ください。

□ 認証デバイスの追加

SMARTACCESS/PremiumV1.1L10 をすでに導入している環境に、認証デバイスを追加する場合は、SMARTACCESS/PremiumV1.1L10 をインストールし直す必要があります

1 バックアップツールで、環境設定情報や全ユーザーのデータを退避します。

バックアップツールについては、『SMARTACCESS/Premium リファレンスガイド ツール編』をご覧ください。

2 SMARTACCESS をアンインストールします。

アンインストールについては、「アンインストール」－「SMARTACCESS をアンインストールする」（→ P.104）をご覧ください。

3 追加する認証デバイスをインストールします。

認証デバイスのインストールについては、「認証デバイスのインストール」（→ P.51）をご覧ください。

4 SMARTACCESS をインストールします。

SMARTACCESS のインストールについては、「SMARTACCESS のインストール」（→ P.54）をご覧ください。

5 バックアップツールで、環境設定情報や全ユーザーのデータを復元します。

POINT

- バックアップツールによるデータの復元後は、認証パターンの設定は前の環境の設定が引き継がれるため、追加した認証デバイスをそのまま使用することはできません。追加した認証デバイスをお使いになる場合は、認証パターンを設定し直してください。
- SMARTACCESS/PremiumV1.1L10がインストール済みの環境でSMARTACCESS/PremiumV1.1L10の setup.exe を実行すると、アンインストールが開始されます。
- アップグレード時には、すでに導入済みの認証デバイスをアンインストールしないでください。SMARTACCESS を正しくアップグレードできない場合があります。
- アップグレード時には、すでにインストールされているツールをカスタマイズインストールによりインストールしない設定にすることはできません。カスタマイズインストールについては『SMARTACCESS/Premium リファレンスガイド カスタマイズ編』をご覧ください。
- バックアップツールにより指紋の個別ユーザー情報は退避されません。指紋の運用モードで「パーソナル運用モード」を使用時に「認証デバイスの追加」を実行する場合は、データの退避を実行する前に必ず「通常運用モード」または「モバイル運用モード」で「個別ユーザー情報を使用」を「しない」に設定してください。「パーソナル運用モード」に設定を戻す場合は、データの復元後に「パーソナル運用モード」にし、個別ユーザー情報を取得し直してください。

5 SMARTACCESS のツール

SMARTACCESS のインストールが完了すると、「環境設定」と「ユーザー情報設定」の 2 つのツールがお使いになれます。

環境設定

「環境設定」は、管理者が SMARTACCESS を利用するセキュリティ環境の設定を管理するためのツールです。
「環境設定」で設定する機能は次のとおりです。

■ ログオン認証

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

Windows ログオン、アプリケーションログオンおよび認証パターンなどの設定をします。

■ ポリシー

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

SMARTACCESS ツールの起動制限や認証デバイスごとのセキュリティ設定をします。

■ 機器制限

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

Portshutter や FENCE-G（SMARTACCESS/Premium のみ）の設定をします。

■ 連携

□ 対象製品

・SMARTACCESS/Premium

□ 設定内容

ActiveDirctory や Systemwalker との連携を設定します。

■ 利用ログ管理

□ 対象製品

・SMARTACCESS/Premium

□ 設定内容

ログ取得に関する設定をします。

■ ユーザー情報管理

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

アカウントおよび認証情報の登録や管理をします。

ユーザー情報設定

「ユーザー情報設定」は、指紋などの情報やパスワードなど、利用者固有の設定を利用者自身が設定するためのツールです。
「ユーザー情報設定」で設定する機能は次のとおりです。

■ ログオン情報の登録

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

BIOS、Windows、およびアプリケーションのログオン情報を登録したり変更したりします。

■ 証明書

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

スマートカードの証明書を登録します。

■連携

□ 対象製品

・SMARTACCESS/Premium

□ 設定内容

FENCE-G や Systemwalke との連携情報を登録したり変更したりします（「環境設定」で、FENCE-G や Systemwalker を利用する設定をした場合に表示されます）。

■ユーザー情報の管理

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

□ 設定内容

利用者のアカウント、および認証情報を登録したり変更したりします。

SMARTACCESS をお使いになる前に

■Windows アカウントのパスワード設定

SMARTACCESS の管理者および利用者には、Windows アカウントにパスワード設定が必要です。
既存の Windows アカウントを SMARTACCESS でお使いになる場合は、あらかじめ Windows でパスワードの設定をします。
新規に Windows アカウントを作成する場合は、SMARTACCESS の「環境設定」で Windows アカウントとパスワードの設定ができます（→ P.73）。

重要

▶ Windows のパスワード設定については、Windows のヘルプをご覧ください。

■ご購入時の設定について

認証デバイスには、ご購入時にユーザー名やパスワード、PIN があらかじめ設定されていますが、セキュリティ上、使い始めるときには必ずパスワードや PIN を変更してください（→『SMARTACCESS/Premium リファレンスガイド　ツール編』、または『SMARTACCESS/Basic リファレンスガイド　ツール編』）。

認証デバイスのご購入時の設定は次のとおりです。

認証デバイス	設定項目	ご購入時の設定
セキュリティチップ	所有者パスワード	administrator
指紋センサー	指紋ユーザー名	saadmin
指紋センサー	バイオパスワード	administrator
IC カード（FeliCa 方式）	利用者 PIN	0000 注
IC カード（FeliCa 方式）	管理者 PIN	administrator 注
スマートカード	利用者 PIN	0000 注
スマートカード	管理者 PIN	administrator 注

注：FMV オプション製品である FeliCa 対応非接触 IC カード（FMFLC-C1）およびスマートカード（FMSMA-C1）を使用した場合の設定値です。それ以外のカードで作成や発行を行った場合はこの限りではありません。

重要

- すでにセキュリティチップの所有者パスワードが設定されている場合、設定されている所有者パスワードが有効になります。

■ Windows XP の「共有とセキュリティ」をお使いの場合

Windows XP の「共有とセキュリティ」をお使いで、ユーザープロファイルのフォルダを「プライベート」に設定している場合は、ユーザープロファイルのフォルダへのアクセスは利用者のみに許可されます。
SMARTACCESS の設定を行うとき、管理者が利用者のユーザープロファイルのフォルダにアクセスする必要があることがありますので、「このフォルダをプライベートにする」の設定をオフにしてください。
設定をオフにする手順は次のとおりです。

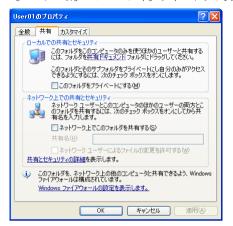
重要

- 「このフォルダをプライベートする」設定を変更するには、管理者権限をもつアカウントでログオンしている必要があります。
- ユーザープロファイルやフォルダのプライベート設定については、Windows のヘルプをご覧ください。

1 **「スタート」ボタン→「マイコンピュータ」の順にクリックします。**
「マイコンピュータ」ウィンドウが表示されます。

2 **Windows がインストールされているドライブ（通常は「ローカル ディスク（C:)」）→「Document and Settings」の順にダブルクリックします。**

3 設定を変更するユーザーアカウント名のフォルダを右クリックし、「共有とセキュリティ」をクリックします。

「[ユーザー名] のプロパティ」ウィンドウが表示されます。

「このフォルダをプライベートにする」のチェックを外します。

4 「OK」をクリックし、すべてのウィンドウを閉じます。

重要

- 運用上の都合などで「このフォルダをプライベートにする」をチェックしている場合、管理者は次の設定ができなくなります。
  - ・「環境設定」－「ユーザー情報管理」の「アカウント追加」
  - ・「環境設定」－「ユーザー情報管理」－「セキュリティチップ」の「ユーザー情報設定の起動」
  - ・「ユーザー情報設定」

環境設定の起動

「環境設定」を起動するには、SMARTACCESS をインストールした管理者権限をもつアカウントで Windows にログオンする必要があります。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

左側の、機能をツリー構造で表示している領域を「設定項目一覧」と呼び、右側には「設定項目一覧」から選択した機能の設定内容を表示します。

「設定項目一覧」には、導入されてない認証デバイスや、インストールされていない連携ソフトウェアは表示されません。また、設定内容にはコンピュータ全体の設定が表示されます。

POINT

- 「設定項目一覧」から選択した機能を設定したら「適用」をクリックし、続けて他の機能を設定することができます。
- 「環境設定」を終了するには、「OK」をクリックします。設定を変更した場合は再起動が要求されます。再起動することで設定を有効にすることができます。

ユーザー情報設定の起動

「ユーザー情報設定」では利用者自身の設定内容の確認や設定を行います。

重要

- 「環境設定」で設定されている認証デバイスによる認証が要求されます。
  「ユーザー情報設定」をお使いになる前に、必ず「セキュリティ環境の構築」（→ P.71）の手順に従って、「環境設定」で利用者のアカウントと認証情報を登録してください。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。**

認証を要求するウィンドウが表示されます。

・例：指紋センサーをお使いの場合の認証要求ウィンドウ

2 認証情報を入力し、ログインします。

認証情報は利用する認証デバイスによって異なります。
「ユーザー情報設定」が起動します。

3 ログオン認証された利用者のユーザー情報が表示されます。

左側の、機能をツリー構造で表示している領域を「設定項目一覧」と呼び、右側には「設定項目一覧」から選択した機能の設定内容を表示します。
「設定項目一覧」には、導入されてない認証デバイスやインストールされていない連携ソフトウェアは表示されません。また、設定内容には「環境設定」で設定されている利用者固有の設定内容が表示されます。

POINT

- 「ユーザー情報設定」を終了するには、「閉じる」をクリックします。

6 セキュリティ環境の構築

セキュリティ環境の構築は、管理者が「環境設定」で行います。また、利用者固有の情報設定は利用者が「ユーザー情報設定」で行います。
SMARTACCESS によるセキュリティ環境の構築手順を例に、基本的な流れを説明します。

ここでは指紋認証を例にとり、コンピュータの起動時および Web サイトの接続時の認証を指紋認証に設定する手順を説明します。
スマートカードなどの認証デバイスをお使いになる場合も、同様の手順で設定します。
セキュリティ構築手順の基本的な流れは次のとおりです。

■ 必須の設定　□ 認証デバイスまたは必要に応じて登録、設定します。

認証パターンの登録の確認
ログオン認証－組み合わせ（複数の認証デバイスの利用の場合）（→ P.72）

↓

アカウントの登録　ユーザー情報管理－アカウントの追加－管理者ウィザード　（→ P.73）

- **SMARTACCESS アカウントの登録　－ SMARTACCESS アカウントの登録**

↓

- **Windows ユーザーの登録　－ Windows ユーザーの登録**

↓

- アカウント登録のための認証
－指紋認証／カードセット要求（セキュリティチップの場合は必要なし）

↓

Windows ログオン　ログオン認証－ Windows ログオン　（→ P.81）

- **Windows ログオンの有効化　－ SMARTACCESS による Windows ログオン**

↓

アプリケーションログオン　ログオン認証－アプリケーションログオン　（→ P.82）

- アプリケーションログオンの有効化　－アプリケーションログオン機能の利用

↓

- パスワード入力画面の登録
－登録されているアプリケーション－パスワード入力画面登録ツール

重要

- 複数の認証デバイスをお使いになる場合は、認証パターンの組み合わせや認証する順序および認証方式を「認証パターンの追加 / 変更」ウィンドウで登録します（→『SMARTACCESS/Premium リファレンスガイド　機能編』、または『SMARTACCESS/Basic リファレンスガイド　機能編』の「ログオン認証」－「ログオン認証の設定方法」）。
- 認証用のユーザー情報の登録は、指紋センサーをお使いの場合は利用者ごとに指紋を登録します。
- 「アプリケーションログオン」を設定した場合は、利用者は「ユーザー情報設定」でアプリケーションログオン情報の登録を行います（→ P.96）。

認証パターンの登録の確認

認証パターンには、ドライバがインストールされている認証デバイスが自動的に登録され、一覧で表示されます。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が起動します。

2 **「設定項目一覧」から「ログオン認証」をクリックします。**

「認証パターン」の一覧にドライバをインストールした認証デバイスが表示されていること確認します。

3 **「キー設定」の（Ctrl+Alt+Delete）の隣に「指紋」が表示されていることを確認します。**

「指紋」以外の認証パターンが表示されている場合には、次の手順で認証パターンを変更します。

1. （Ctrl+Alt+Delete）をクリックして選択し、「編集」をクリックします。
   「認証パターンの追加／変更」が起動します。

2. 「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が空白の組合せをクリックして「OK」をクリックします。

重要

- 「キー設定」は、「Windows へようこそ」ウィンドウから認証ウィンドウに切り換えるときに使われるキーです。ご購入時の設定は「（Ctrl+Alt+Delete）」が登録されていますが、必要に応じて変更することができます。
  変更するには、「編集」をクリックし、「認証パターンの追加 / 変更」ウィンドウで行います（→『SMARTACCESS/Premium リファレンスガイド　機能編』、または『SMARTACCESS/Basic リファレンスガイド　機能編』の「ログオン認証」－「ログオン認証の設定方法」）。
- スマートカードホルダーが外された状態で SMARTACCESS のインストールすると、「認証パターン」に「スマートカード」が登録されません。その場合は、いったん SMARTACCESS をアンインストールしてからスマートカードホルダーを取り付けて再度 SMARTACCESS をインストールしてください。

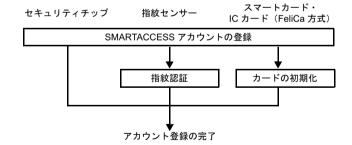
4 **続けてアカウントの登録を行う場合は、「適用」をクリックします。**

アカウントの登録を行う場合は、「アカウントの登録」（→ P.73）をご覧ください。

POINT

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

アカウントの登録

SMARTACCESS を利用する管理者や利用者のアカウントは、「管理者ウィザード」で登録します。
お使いの認証デバイスによってアカウントの登録の手順は異なります。「管理者ウィザード」利用したアカウントの登録手順は次のとおりです。

重要

- 「環境設定」の「ポリシー」でパスワードの複雑さなどが設定されている場合は、そのパスワード制限に準じます。
- スタンドアロンまたはワークグループ環境で利用しているコンピュータの場合、Windows アカウントは Administrators グループに所属している必要があります。
- ドメイン環境で利用しているコンピュータの場合、Windows アカウントは、ActiveDirectory（ドメインコントローラ）の Domain Admins グループに所属している必要があります。
- 指紋センサーをお使いの場合、「環境設定」でのアカウントの登録後に利用者自身の指紋を登録する必要があります（→ P.89）。
- SMARTACCESS/Premium でバイオ認証装置連携をお使いの場合、SMARTACCESS アカウントの「アカウント名」と「パスワード」は、バイオ認証装置に登録されている「ユーザー名」と「パスワード」と同じ情報を登録します。

■管理者と利用者のアカウントの登録

ここでは、指紋センサーを使ったセキュリティ環境で、新規に管理者と利用者を順に登録する手順を説明します。

重要

- 指紋センサーをお使いで、指紋認証をローカルコンピュータで行う場合、アカウントの登録には認証が必要です。アカウントを登録するために、ご購入時の設定で「saadmin」アカウントを用意しています。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が起動します。

2 **「設定項目一覧」から「ユーザー情報管理」をクリックします。**

3 「アカウントの追加」から「起動」をクリックします。

「管理者ウィザード」ウィンドウが表示されます。

4 内容を確認し、「次へ」をクリックします。

「SMARTACCESS アカウントの登録」が表示されます。

5 SMARATACCESS で使用する管理者アカウントを登録します。「アカウント名」と「パスワード」、「パスワード入力確認」を入力して、「次へ」をクリックします。

「Windows ユーザーの登録」が表示されます。

重要

- 「アカウント名」および「パスワード」は SMARTACCESS のアカウント名およびパスワードです。
  アカウント名とパスワードの制限は次のとおりです。
  - ・アカウント名
    - ・指紋センサーの場合
      重複しない 1 ～ 16 文字の半角英数字と記号 $()@_-.%
    - ・その他の認証デバイスの場合
      1 文字以上
  - ・パスワード
    - ・指紋センサーの場合
      8 ～ 32 文字の半角英数字と記号 $()@_-.%
    - ・その他の認証デバイスの場合
      6 ～ 256 文字
- 「ポリシー」で「複雑さの設定」などの制限を設定している場合、設定されている制限に従います。
- 「パスワードの確認」には、「パスワード」と同じ情報を入力します。
- 指紋センサーをお使いになる場合、「アカウント名」は「ユーザー名」、「パスワード」は「バイオパスワード」として設定されます。
- セキュリティチップをお使いになる場合、「パスワード」は「ユーザーキーパスワード」として設定されます。
- スマートカードや IC カード（FeliCa 方式）をお使いになる場合、「パスワード」は「PIN」として設定されます。

6 管理者用の Windows ユーザーを登録します。「Windows ユーザー名」と「ドメイン」、「パスワード」、「パスワード入力確認」を入力し、「次へ」をクリックします。

設定の確認」が表示されます。

重要

- 「Windows ユーザー名」、「パスワード」は、SMARTACCESS アカウントの「アカウント名」、「パスワード」と異なる情報で登録可能です。
- すでに Windows アカウントが登録されている場合、「Windows ユーザー名」の▼をクリックしてユーザー名を選択できます。
- ドメインに参加している場合は、「ドメイン」の▼をクリックしてドメインを選択できます。
- 「ドメイン」を選択してから、「Windows ユーザー名」の▼をクリックするとそのドメインのユーザーアカウントを選択できます。
- 「パスワード」には、Windows アカウントで登録されているパスワードを入力します。
- 「パスワード入力確認」には、「パスワード」と同じ情報を入力します。

POINT

- スマートカードおよび IC カード(FeliCa 方式)の場合は、カードセットを要求するウィンドウが表示されますので、リーダ／ライタにカードをセットします。

7 **「別のユーザーを設定する」をチェックして「次へ」をクリックすると、続けて利用者のアカウントを登録できます。**

「SMARTACCESS アカウントの登録」が表示されます。

複数のアカウントを登録する場合は、手順 5 〜 7 を繰り返します。

8 **アカウントの登録を終了するには、「別のユーザーを設定する」のチェックを外して「次へ」をクリックします。**

「指紋認証」ウィンドウが表示されます。

重要

- スマートカードおよび IC カード（FeliCa 方式）をお使いの場合、カードセットを要求するウィンドウが表示されますので、リーダ／ライタにカードをセットします。「完了」と表示されます。手順 11 に進んでください。
- セキュリティチップをお使いの場合は、「完了」と表示されます。手順 11 に進んでください。

9 【F10】キーを押します。

「ユーザー名とバイオパスワードを入力してください。」と表示されます。

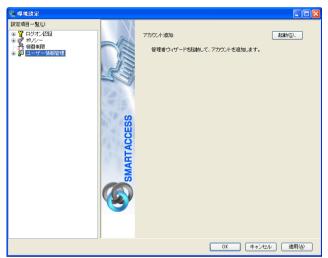
10 指紋認証をローカルコンピュータで行う場合は、「ユーザー名」に「saadmin」、「バイオパスワード」に「administrator」と入力し、「OK」をクリックします。

「完了」と表示されます。

重要

- ユーザー名「saadmin」は、指紋認証をローカルコンピュータで行われる場合に利用する、ご購入時の指紋認証用の管理者アカウントです。
  管理者の登録完了後、ユーザー名「saadmin」を削除することをお勧めします。(→『SMARTACCESS/Premium リファレンスガイド　ツール編』または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「管理者ツール」－「ユーザー情報管理」－「指紋」)

11 「完了」をクリックします。

「環境設定」に戻ります。

12 続けて Windows ログオンの設定を行う場合は、「適用」をクリックします。

Windows ログオンの設定を行う場合は、「Windows ログオン」(→ P.81)をご覧ください。

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

Windows ログオン

SMARTACCESS は Windows へのログオンを、認証デバイスを利用したログオンに置き換えることができます。
ここでは、Windowsのログオン認証を従来のWindowsパスワードの認証からSMARTACCESSのデバイス認証に変更する手順を説明します。

■ Windows ログオンの有効化

Windows ログオンを利用するには、「SMARTACCESS による Windows ログオン」を有効にします。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。

3 「SMARTACCESSによるWindowsログオン」を「する」をクリックします。

4 続けてアプリケーションログオンの設定を行う場合は、「適用」をクリックします。

アプリケーションログオンの設定を行う場合は、アプリケーションログオンの有効化に進みます（→ P.82）

POINT

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

アプリケーションログオン

「アプリケーションログオン」は、アプリケーションの起動時や Web サイトへの接続時のパスワード認証を SMARTACCESS で認証する機能です。

重要

- 「環境設定」で「アプリケーションログオン」を設定した場合、利用者は「ユーザー情報設定」で「アプリケーションログオン情報」を登録することにより Web サイトへのアプリケーションログオンを行うことができます（→ P.96）。

■アプリケーションログオンの有効化

Internet Explorer で表示される Web サイトのパスワード認証を、SMARTACCESS のデバイスによる認証に置き換える手順を説明します。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ログオン認証」→「アプリケーションログオン」の順にクリックします。

3 「アプリケーションログオン機能の利用」の「する」をクリックします。

4 続けてパスワード入力画面の登録を行う場合は、「適用」をクリックします。

パスワード入力画面の登録を行う場合は、「パスワード入力画面の登録」（→ P.83）をご覧ください。

POINT

▶「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

■パスワード入力画面の登録

Internet Explorer で表示される Web サイトのパスワード認証を、SMARTACCESS のデバイスによる認証に置き換える手順を説明します。

重要

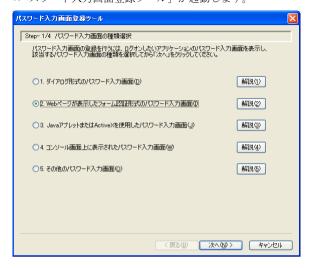
▶「アプリケーションログオン」で関連付けする Web サイトは、認証サービスに対応している必要があります。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ログオン認証」→「アプリケーションログオン」の順にクリックします。

3 「全ユーザー共通のパスワード入力画面情報ファイルの参照先」に参照先のフォルダが表示されていることを確認してから、「新規」をクリックします。

「パスワード入力画面登録ツール」が起動します。

POINT

- 参照先を変更するには、「参照」をクリックして、インストール先のフォルダを変更してください。
- 「全ユーザー共通のパスワード入力画面情報ファイルの参照先」は SMARTACCESS の「パスワード入力画面」の設定情報を記述したファイルを格納するフォルダです。必要に応じて格納先を変更することができます。

4 Internet Explorerを起動し、Webサイトに接続してパスワード入力画面を表示します。

重要

- 「Web ページが表示したフォーム認証形式のパスワード入力画面」をお使いになる場合は、ブラウザソフトは Internet Explorer をお使いください。他のブラウザソフトをお使いになる場合は、「Java アプレットまたは ActiveX を使用したパスワード入力画面」を選択します（→『SMARTACCESS/Premium リファレンスガイド　機能編』、または『SMARTACCESS/Basic リファレンスガイド　機能編』の「アプリケーションログオン」－「パスワード入力画面の登録」）。

5 「Web ページが表示したフォーム認証形式のパスワード入力画面」をクリックして、「次へ」をクリックします。

「Step-2/4 表題の指定」と表示されます。

POINT

- 接続した Web サイトのパスワード入力画面に「パスワード入力画面登録ツール」ウィンドウが隠れている場合は、タスクバーなどで「パスワード入力画面登録ツール」ウィンドウをアクティブにします。

6 「関連付けツール」を Web サイトの表題にドラッグし、パスワード入力画面の表題を指定します。

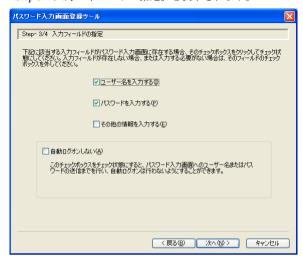
「表題」「URL」にドラッグした Web サイトのパスワード入力画面のタイトルと URL が入力されます。

POINT

- 次の例のように「関連付けツール」を Web サイトのパスワード入力画面のタイトルバーにドラッグします。

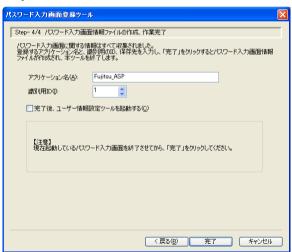
「関連付けツール」は関連付けすると、表示が から に変わります。

7 内容を確認して、「次へ」をクリックします。

「Step-3/4 入力フィールドの指定」と表示されます。

POINT

- Web サイトの入力フィールドがパスワードのみの場合は「パスワードを入力する」だけにチェックをしてください。

8 「ユーザー名を入力する」と「パスワードを入力する」にチェックが入っていることを確認して、「次へ」をクリックします。

「Step-4/4 パスワード入力画面情報ファイルの作成、作業完了」と表示されます。

9 「アプリケーション名」を入力して、「完了」をクリックします。

「パスワード入力画面情報が登録されました。」という確認ウィンドウが表示されます。

10 「OK」をクリックして、「環境設定」に戻ります。

登録したWebサイトを表示しているInternetExplorerのウィンドウを閉じてください。

11 「OK」をクリックして、「環境設定」を終了します。

再起動を要求するウィンドウが表示されます。

POINT

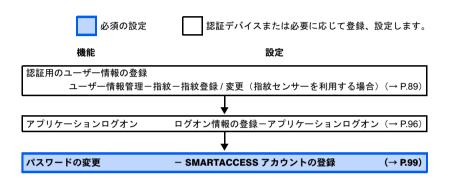
- 続けて他の機能の設定を行う場合は、「適用」をクリックします。

12 「はい」をクリックして Windows を再起動し、設定を有効にします。

重要

- Internet Explorer のクロススクリプティング問題への対策により、パスワード入力画面が frame タグを使用してほかの URL を参照している場合、正しくログオンできない場合があります。この場合、参照先の URL をインターネットオプションで「信頼済みサイト」として登録しておく必要があります。

7 利用者固有のセキュリティ情報の設定

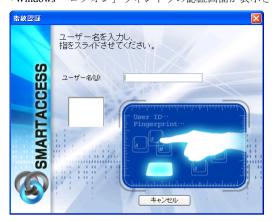
管理者が「環境設定」で構築したセキュリティ環境は提供されますが、利用者がSMARTACCESS の運用開始時に利用者固有のセキュリティ情報を設定します。
ここでは、「セキュリティ環境の構築」（→ P.71）で構築されたセキュリティ環境を利用するための利用者の認証情報やパスワード設定する手順を説明します（例として指紋センサーを利用した場合を記述します）。

認証用のユーザー情報の登録

指紋センサーをお使いになる場合は、認証用の指紋の登録が必要です。指紋の登録は、「ユーザー情報設定」で行います。

1 コンピュータを起動します。

「Windows へようこそ」ウィンドウが表示されます。

2 【Ctrl】+【Alt】+【Delete】キーを押します。

「Windows へログオン」ウィンドウの認証画面が表示されます。

3 【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「Windows へログオン」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。

4 「ユーザー名」「バイオパスワード」を入力して、「OK」をクリックします。

Windows が起動します。

重要

- 指紋を登録する利用者アカウントのユーザー名とバイオパスワードを入力します（→ P.92）。

5 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。**

「ユーザー情報設定」ウィンドウの認証画面が表示されます。

6 **【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。**

「ユーザー情報設定」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。

7 「バイオパスワード」を入力して、「OK」をクリックします。

「ユーザー情報設定」ウィンドウが表示されます。

重要

- 指紋を登録する利用者アカウントのバイオパスワードを入力します。

8 「設定項目一覧」から「ユーザー情報管理」→「指紋」の順にクリックします。

起動時に認証したアカウントの指紋情報が表示されます。

9　内容を確認して、「登録」をクリックします。

「指紋認証」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。

10　【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「指紋認証」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。

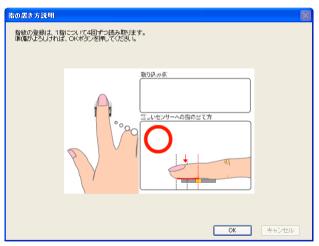
11 「バイオパスワード」を入力して、「OK」をクリックします。

「指紋の登録／変更」ウィンドウが表示されます。

重要

- 指紋を登録する利用者アカウントのバイオパスワードを入力します（→ P.92）。

12 指紋を登録したい指をクリックして、「登録／変更」をクリックします。

「指の置き方説明」ウィンドウが表示されます。

POINT

- 間違えて別の指をクリックした場合は、「キャンセル」をクリックして再度「登録／変更」をクリックし直します。

13 内容を確認して、「OK」をクリックします。

「指紋入力」ウィンドウが表示されます。

14 表示されるメッセージに従って、4 回指紋を入力し、「登録する指紋データを作成しました」と表示されたのを確認して「OK」をクリックします。

「指紋の登録／変更」ウィンドウが表示されます。

15 **2 本目に登録する指をクリックし、手順 12 ～ 14 の操作を行います。**

「指紋の登録 / 変更」ウィンドウが表示されます。

16 **登録した指にチェックマークが設定されていることを確認し、「OK」をクリックして、指紋情報を登録します。**

「ユーザー情報設定」ウィンドウに戻ります。

POINT

- 登録した指紋を取り消すには、登録した指をクリックして「削除」をクリックします。
- 「キャンセル」をクリックすると指紋の登録を中断して「ユーザー情報設定」ウィンドウに戻ります。

続けて「アプリケーションログオン情報」の登録を行う場合は、「アプリケーションログオン情報の登録」（→ P.96）をご覧ください。

POINT

- 「ユーザー情報設定」を終了するには、「閉じる」をクリックします。

アプリケーションログオン情報の登録

利用者のアプリケーションログオン情報の登録を行います。

重要

- 「アプリケーションログオン情報」を登録するには、「アプリケーションログオン」を利用する利用者アカウントで Windows にログオンする必要があります。
- 「アプリケーションログオン」を利用する利用者アカウントで、「ユーザー情報設定」を起動するときは利用者アカウントで認証します。
- 「アプリケーションログオン情報」を登録するには、事前に管理者が「環境設定」で「アプリケーションログオン」の設定を行っている必要があります。

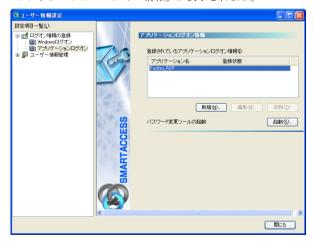
1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

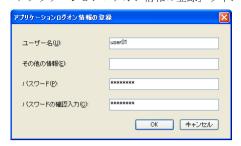
「ユーザー情報設定」ウィンドウの認証画面が表示されます。

2 ウィンドウのメッセージに従って指紋を入力します。

認証されると「ユーザー情報設定」が起動します。

3 「設定項目一覧」から「ログオン情報登録」→「アプリケーションログオン」の順にクリックします。

「アプリケーションログオン情報」が表示されます。

4 登録するアプリケーション名をクリックして、「新規」をクリックします。

「アプリケーションログオン情報の登録」ウィンドウが表示されます。

POINT

- 「登録されているアプリケーションログオン情報」には、管理者が「環境設定」で構築したアプリケーションログオン情報が一覧で表示されます。

5 「ユーザー名」「パスワード」「パスワードの確認入力」を入力して、「OK」をクリックします。

「ユーザー情報設定」ウィンドウに戻ります。

登録が完了すると「登録されているアプリケーションログオン情報」のリストの「登録状態」の表記が「登録済み」と表示されます。

重要

- 「ユーザー名」「パスワード」には、Web サイトにログオンするときに必要なユーザー名とパスワードを入力します。

POINT

- 登録しているアプリケーションが「Web　ページが表示したフォーム認証形式のパスワード入力画面」などの場合、「その他の情報」に入力する必要はありません。

6 続けてパスワードの変更を行う場合は、「パスワードの変更」（→ P.99）をご覧ください。

POINT

▶「ユーザー情報設定」を終了するには、「閉じる」をクリックします。

パスワードの変更

利用者がパスワードの変更をすることで、パスワードを知っているのは利用者本人だけになります。セキュリティを強化するためにも、SMARTACCESS 運用開始時に利用者がパスワードを変更することをお勧めします。

アカウントには、「Windows アカウント」と認証デバイスで利用する「SMARTACCESS アカウント」があります。SMARTACCESS の運用を開始すると、ログオン時に入力するアカウント情報は、認証デバイスで利用するアカウントになります。
ここでは、指紋センサーで利用するアカウントのバイオパスワードの変更をご説明します。

重要

▶ 利用者がパスワードを変更するには、利用者アカウントで Windows にログオンする必要があります。
また、「ユーザー情報設定」を起動するときは利用者アカウントで認証します。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

「ユーザー情報設定」ウィンドウの認証画面が表示されます。

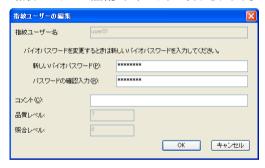
2 ウィンドウのメッセージに従って指紋を入力します。

認証されると「ユーザー情報設定」が起動します。

3 「設定項目一覧」から「ユーザー情報管理」→「指紋」の順にクリックします。

起動時に認証したアカウントの指紋情報が表示されます。

4 「編集」をクリックします。

「指紋ユーザーの編集」ウィンドウが表示されます。

5 「新しいバイオパスワード」「パスワードの確認入力」を入力し、「OK」をクリックします。

「ユーザー情報設定」ウィンドウに戻ります。

重要

- 指紋センサーのバイオパスワード制限は、8～32文字の半角英数字と記号$()@_-.%です。指紋センサー以外の認証デバイスのパスワード制限は6～256文字です。
- 「ポリシー」で複雑さの設定を行っている場合は、設定されているパスワード制限に従って指定します。

6 「閉じる」をクリックして、「ユーザー情報設定」を終了します。

重要

- 利用者が Windows アカウントのパスワードを変更するには、「ユーザー情報設定」で「ログオン情報登録」→「Windows ログオン」の「編集」をクリックして表示される、「Windows ログオン情報の変更」ウィンドウで行います(→『SMARTACCESS/Premium リファレンスガイド　ツール編』、または『SMARTACCESS/Basic リファレンスガイド　ツール編』の「利用者ツール」－「ログオン情報の登録」－「Windows ログオン」)。

8 SMARTACCESS の利用

管理者および利用者によるセキュリティ環境の構築が完了すると、利用者はSMARTACCESS の機能を利用することができます。

Windows ログオン

ここでは、指紋センサーを利用して Windows ログオンをする手順を説明します。

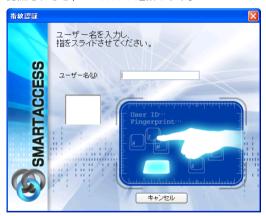
1 コンピュータを起動します。

「Windows へようこそ」ウィンドウが表示されます。

2 【Ctrl】+【Alt】+【Delete】キーを押します。

「Windows へログオン」ウィンドウの認証画面が表示されます。

3 ウィンドウのメッセージに従って「ユーザー名」を入力して、指紋を入力します。

認証されると、Windows が起動します。

重要

- 「ユーザー名」には、認証デバイスで利用する「SMARTACCESS アカウント」を入力します。

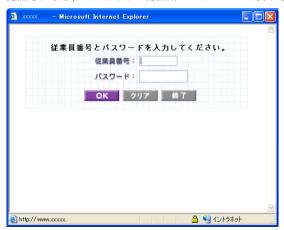
アプリケーションログオン

ここでは、Internet Explorer 経由で Web サイトの接続したときに指紋センサーを利用して認証する手順を説明します。

1 Internet Explorer を起動して、Web サイトに接続します。

「アプリケーションログオン」ウィンドウが表示されます。

2 ウィンドウのメッセージに従って、指紋を入力します。

認証されると、Web サイトの認証用の Web ページが表示されます。

3 Web サイトにログオンするときの認証情報を入力して、認証します。

9 アンインストール

SMARTACCESS をアンインストールする

SMARTACCESS のアンインストールは、次の手順で行います。

重要

- アンインストールをするには､SMARTACCESS をインストールした管理者権限をもつアカウントでログオンしている必要があります。
- 暗号化したファイルやメールなどがある場合は、暗号化を解除してからアンインストールを行ってください。
- 再起動の要求があった場合は、必ず再起動を行ってください。

1 「スタート」ボタン→「コントロールパネル」の順にクリックします。

「コントロールパネル」ウィンドウが表示されます。

2 次の操作をします。

■ Windows XP の場合

「プログラムの追加と削除」をダブルクリックします。

■ Windows 2000 の場合

「アプリケーションの追加と削除」をダブルクリックします。

3 「SMARTACCESS」をクリックし、「削除」をクリックします。

この後は、メッセージに従って操作します。

認証デバイスのアンインストール

認証デバイスのドライバのアンインストールは、「コントロールパネル」の「プログラムの追加と削除（Windows2000 の場合は、アプリケーションの追加と削除）」で行います。

■アンインストール時の注意事項

□ セキュリティチップ

- セキュリティチップをアンインストールする場合は、必ず SMARTACCESS をアンインストールした後で行ってください。
  セキュリティチップをアンインストールした状態で、SMARTACCESS によるログオンを行うと、Windows が正常に起動できなくなります。
- セキュリティチップをアンインストールするには、管理者権限で Windows にログオンする必要があります。
- 再起動の要求があった場合は、必ず再起動を行ってください。

□ FeliCa 対応リーダ／ライタ

・Sony FeliCa リーダ／ライタをアンインストールする場合は、必ず SMARTACCESS/Premium をアンインストールした後で行ってください。
Sony FeliCa リーダ／ライタをアンインストールした状態で、SMARTACCESS/Premium によるログオンを行うと、Windows が正常に起動できなくなります。
・FeliCa リーダー／ライターソフトウェアをアンインストールするには、管理者権限で Windows にログオンする必要があります。
・再起動の要求があった場合は、必ず再起動を行ってください。

第 5 章

ネットワーク運用

本製品では、ネットワークを利用して SMARTACCESS のセキュリティ環境を集中管理することができます。
この章では、「Active Directory 連携」と「バイオ認証装置連携」の導入を説明しています。
なお、ネットワーク運用は SMARTACCESS/Premium でお使いになれる機能です。
Active Directory 連携、バイオ認証装置連携については、『SMARTACCESS/Premium リファレンスガイド　機能編』をご覧ください。

1 Active Directory 連携

「Active Directory連携」をWindowsドメイン環境に導入することで、SMARTACCESS設定情報をActive Directoryサーバーで集中管理することができます。これによりドメイン管理者の負担を軽減し、企業コンピュータ環境のSMARTACCESSでのセキュリティ環境の標準化を維持することができます。

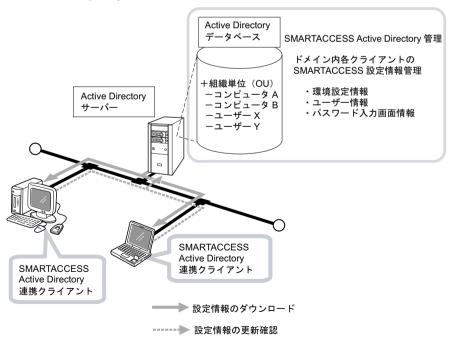
「Active Directory 連携」には、次のツールが準備されています。

■ SMARTACCESS Active Directory 管理

SMARTACCESS Active Directory 管理（以下、Active Directory 管理）は、個々のコンピュータ上にある SMARTACCESS のセキュリティ環境を集中管理します。
「Active Directory 管理」が管理できる情報は次のとおりです。

- 環境設定情報
- ユーザー情報（Windows ログオン情報やアプリケーションログオン情報など）
- パスワード入力画面情報

■ SMARTACCESS Active Directory 連携クライアント

SMARTACCESS Active Directory 連携クライアント（以降、Active Directory 連携クライアント）は、設定情報の適用が必要かどうかを定期的に確認し、適用が必要な場合は「SMARTACCESS 更新確認」ウィンドウを表示してセキュリティ環境を新しい設定に適用させることができます。

Active Directory 連携の導入準備

Active Directory 連携を導入するには、次の条件を満たしている必要があります。

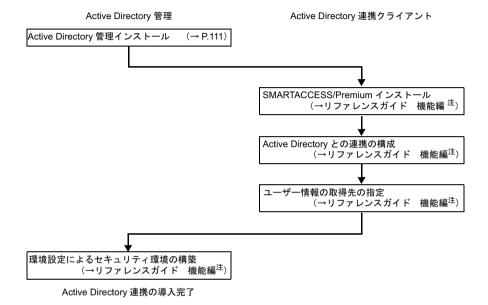
■ システムの必要条件

項目	Active Directory 管理	Active Directory 連携クライアント
ハードディスク	70MByte 以上の空き容量	50MByte 以上の空き容量
OS	Windows 2000 Server 以上	Windows 2000 以上
Windows ドメイン	Active Directory サーバー（ドメインコントローラ）	Windows ドメインクライアント
サービス	Active Directory	—
SMARTACCESS	SMARTACCESS/Premium	

重要

- 「Active Directory管理」は、連携したActive Directoryが管理するドメインが管理対象になります。
- 「Active Directory 連携クライアント」のコンピュータは、ドメインに参加している必要があります。
- Active Directory のユーザーや組織単位（OU）は、Active Directory での登録が必要です。Active Directory については、Windows Server のヘルプをご覧ください。

Active Directory 連携の導入ステップ

Active Directory 連携を導入するには、Active Directory サーバーに「Active Directory 管理」、クライアントコンピュータに「Active Directory 連携クライアント」を導入します。主な導入手順は次のとおりです。

注：『SMARTACCESS/Premium リファレンスガイド　機能編』の「Active Directory 連携」

Active Directory 管理のインストール

「Active Directory 管理」のインストールは、インストーラを実行して画面の指示に従いながら行います。

重要

- 「Active Directory 管理」のインストールをするには、ドメイン管理者権限で Windows にログオンしている必要があります。
- 「Active Directory 管理」をインストールする前に、使用中のアプリケーションはすべて終了させてください。
- ハードディスクに十分な空容量があることをご確認ください。

1 「SMARTACCESS/Premium」CD-ROM をセットします。

2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。

3 「名前」に次のように入力し、「OK」をクリックします。

[CD/DVDドライブ]:¥SAPremium¥Active Directory¥Setup¥setup.exe

「SMARTACCESS Active Directory 管理の InstallShield ウィザードへようこそ」と表示されます。

4 「次へ」をクリックします。

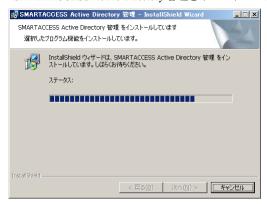
「インストール先のフォルダ」と表示されます。

5 インストール先を確認し、「次へ」をクリックします。

インストール先を変更する場合は、「変更」をクリックして別のインストール先フォルダを指定します。

「プログラムがインストールできる準備ができました」と表示されます。

6 「インストール」をクリックして、インストールを開始します。

「SMARTACCESS Active Directory 管理をインストールしています」と表示されます。

インストールが正常に完了すると、「Install Shield ウィザードを完了しました」と表示されます。

7 「完了」をクリックします。

再起動を要求するメッセージが表示されます。

8 「はい」をクリックして、Windows を再起動します。

「Active Directory 管理」のインストール情報を有効にするには、Windows の再起動が必要です。

重要

- Active Directory 管理から環境設定を行う場合、あらかじめ SMARTACCESS/Premium V1.1L10 がインストールされている環境で初期値の情報を準備する必要があります。
  操作手順は次の通りです。
  1. SMARTACCESS/Premium V1.1L10 がインストールされている環境で、「バックアップツール」を使用してバックアップを作い「環境設定ファイル（F5FZCFGM.fcb）」を作成します（→『SMARTACCESS/Premium リファレンスガイド　ツール編』）。
  2. 「バックアップツール」で作成した「環境設定ファイル」を「Active Directory 管理」がインストールされたフォルダに格納します。
     格納先は次の通りです。
     C:¥Program Files¥Fujitsu¥SMARTACCESS¥Data
     なお、インストール時にインストールフォルダを変更した場合は、変更先のインストールフォルダにある「¥Data」に格納してください。
  3. 「Active Directory 管理」から環境設定を行います。

2 バイオ認証装置連携

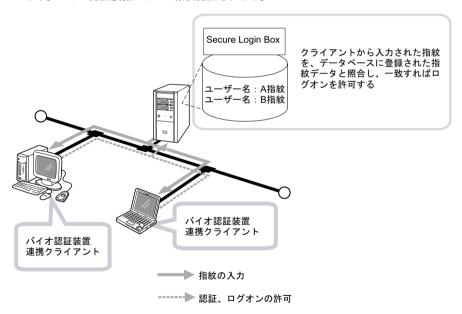
バイオ認証装置連携は、「バイオ認証装置 Secure Login Box」で管理された指紋による認証（バイオ認証）を SMARTACCESS で実現する機能です。認証デバイスから入力された指紋と、バイオ認証装置が管理する認証用の指紋を照合して本人認証を行います。バイオ認証装置との連携によりユーザーの認証用の指紋を一括管理することができます。

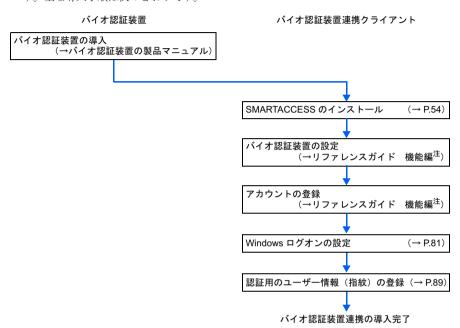
バイオ認証装置連携をお使いになるために必要なものは、次のとおりです。

□ バイオ認証装置

認証用の指紋情報を一括管理します。

□ バイオ認証装置連携クライアント

バイオ認証装置のクライアントになるコンピュータは、SMARTACCESS でバイオ認証装置と連携することで、指紋による Windows ログオンやアプリケーションログオンが利用できます。バイオ認証装置によって指紋認証されます。

バイオ認証装置連携の導入

バイオ認証装置連携を導入するには、ネットワーク上にサーバーとしてバイオ認証装置を導入し、「バイオ認証装置連携クライアント」には「SMARTACCESS/Premium」を導入します。主な導入手順は次のとおりです。

注：『SMARTACCESS/Premium リファレンスガイド　機能編』の「Seure Login Box 連携」

重要

- バイオ認証装置の導入については、バイオ認証装置の製品マニュアルをご覧ください。
- 「バイオ認証装置連携クライアント」については、『SMARTACCESS/Premium リファレンスガイド　機能編』の「Seure Login Box 連携」をご覧ください。

第 6 章

運用例

SMARTACCESS には、安全なセキュリティ環境を構築するためのさまざまな認証デバイスの利用やセキュリティ機能があります。
この章では、代表的な認証デバイスを利用するセキュリティ環境の事例をご説明しています。

1 セキュリティチップで暗号化ファイルの鍵を保護

セキュリティチップをお使いになると、電子メールや Windows 暗号化ファイルシステム（EFS）で利用される秘密鍵を保護することができます。

ここでは、セキュリティチップを利用するセキュリティ環境と Windows 暗号化ファイルシステム（EFS）の秘密鍵を保護する設定と利用について説明します。

重要

- Windows 暗号化ファイルシステム（EFS）は、Windows XP Professional および Windows 2000 でサポートされます。
  Windows 暗号化ファイルシステム（EFS）をお使いになる場合は、ハードディスクのファイルシステムは NTFS でフォーマットする必要があります。
- Windows 暗号化ファイルシステム（EFS）を使ってファイルを暗号化する場合は、ファイルまたはフォルダのプロパティで設定します
- Windows XP Home Edition は、暗号化ファイルシステム（EFS）をサポートしておりません。

Windows 暗号化ファイルシステム（EFS）の有効化

セキュリティチップで Windows 暗号化ファイルシステム（EFS）の秘密鍵を保護するには、管理者が利用者ごとに「環境設定」の「ユーザー情報管理」で設定します。
ここでは、セキュリティチップによる Windows 暗号化ファイルシステム（EFS）で必要となる証明書は新規に作成します。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**
「環境設定」が起動します。

2 **「設定項目一覧」から「ユーザー情報管理」→「セキュリティチップ」の順にクリックします。**
セキュリティチップの「ユーザー情報管理」の詳細が表示されます。

3 「Windows アカウント情報」から Windows 暗号化ファイルシステム（EFS）を利用する利用者の「ユーザー名」をクリックし、「初期化」をクリックします。

「ユーザーの初期化」ウィンドウが表示されます。

認証パターンにセキュリティチップが含まれている場合は、管理者ウィザードの実行時にユーザーの初期化が完了していますので「初期化」をクリックすると、「ユーザー初期化ウィザード」が起動します。手順 6 に進んでください。

重要

- 「環境設定」を起動している管理者以外の利用者の「ユーザー名」を選択すると、「セキュリティチップ」ウィンドウが表示されます。初期化する利用者の Windows パスワードを入力してください。

4 「パスワード」および「パスワードの確認入力」にセキュリティチップで使用するユーザーキーパスワードを入力して、「OK」をクリックします。

5 もう一度「初期化」をクリックします。

「ユーザー初期化ウィザード」が起動します。

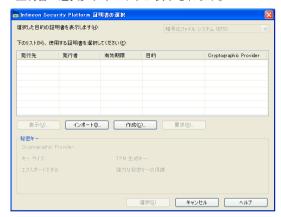
6 「次へ」をクリックします。

「Security Platform の機能－ Security Platform の機能を選択してください」と表示されます。

7 「暗号化ファイルシステム（EFS）によるファイルとフォルダの暗号化」をオンにし、「次へ」をクリックします。

「Security Platform の機能－暗号化証明書」と表示されます。

8 別の証明書を選択するには、「選択」をクリックします。

「証明書の選択」ウィンドウが表示されます。

重要

- セキュリティチュップで Windows 暗号化ファイルシステム（EFS）をお使いになるには証明書が必要です。一覧に表示されている証明書を利用する場合は、証明書を選択して「次へ」をクリックします。

9 新規に証明書を作成するために、「作成」をクリックします。

「ユーザー認証」ウィンドウが表示されます。

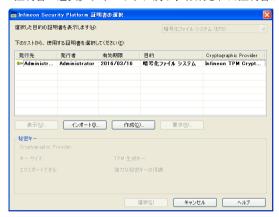
10 「基本パスワードキー」に利用者のユーザーキーパスワードを入力して、「OK」をクリックします。

パスワード確認入力をするための「ユーザー認証」ウィンドウが表示されます。

重要

- 作成済みの証明書をお使いになる場合は、一覧から証明書を選択して「選択」をクリックします。

11 もう一度ユーザーキーパスワードを入力して、「OK」をクリックします。

「証明書の選択」ウィンドウに戻り、作成された証明書がリストに追加されます。

12 「次へ」をクリックします。

「Security Platform の機能－設定を確認してください」と表示されます。

13 「次へ」をクリックします。

「ウィザードが正常に終了しました。」と表示されます。

14 **「完了」をクリックします。**

15 **「環境設定」の「OK」をクリックします。**
続けて他の利用者の設定を行う場合は、「適用」をクリックします。

16 **コンピュータを再起動します。**
Windows を再起動することで設定を有効にします。

Windows 暗号化ファイルシステム（EFS）の利用

Windows 暗号化ファイルシステム（EFS）は、通常の環境と同じように設定して利用することができます。ここでは、セキュリティチップを利用して Windows ログオンし、フォルダに Windows 暗号化ファイルシステム（EFS）の設定をするまでを説明します。
Windows 暗号化ファイルシステム（EFS）については、Windows のヘルプをご覧ください。

■Windows 暗号化ファイルシステム（EFS）の設定

1 **Windows にログオン後、暗号化設定をするフォルダを右クリックして、「プロパティ」をクリックします。**
フォルダのプロパティのウィンドウが表示されます。

2 **「全般」タブの「詳細設定」をクリックします。**
「属性の詳細」ウィンドウが表示されます。

3 **「内容を暗号化してデータをセキュリティで保護する」をオンにし、「OK」をクリックします。**
ファイルまたはフォルダのプロパティのウィンドウに戻ります。

POINT

- 「内容を圧縮してディスク領域を節約する」を併用して設定することはできません。詳しくは、Windows のヘルプをご覧ください。

4 「OK」をクリックします。

「属性の変更の確認」ウィンドウが表示されます

重要

- ファイルの場合は、「暗号化に関する警告」ウィンドウが表示されます。暗号化する対象を選択して、「OK」をクリックします。

5 暗号化する対象を選択して、「OK」をクリックします。

設定が完了すると、フォルダのプロパティのウィンドウが閉じられます。

POINT

- Windows 暗号化ファイルシステム（EFS）を設定したファイルまたはフォルダに他の利用者がアクセスしようとすると、アクセス拒否するメッセージが表示されます。セキュリティチップによる Windows 暗号化ファイルシステム（EFS）を設定したファイルの秘密鍵はセキュリティチップで管理されます。セキュリティチップで管理された秘密鍵を外に持ち出すことはできないので、機密文書などを安全に保護することができます。

2 スマートカードの抜き取りによるコンピュータのロック

スマートカードをお使いになると、Windows にログオンするときにユーザー名やパスワードを入力する代わりにスマートカードをリーダ／ライタにセットすることでログオンできます。

スマートカードをお使いになることにより、パスワードの漏えいの危険がなくなり、コンピュータの不正利用やなりすましを防ぐことができます。また離席時にリーダ／ライタからスマートカードを抜き取るだけでコンピュータをロックすることができます。コンピュータのロックを解除するには、再度リーダ／ライタにスマートカードをセットします。

カードのポーリング動作

ここでは、カード抜き取り時にコンピュータをロックする設定を説明します。

重要

- あらかじめ認証パターンの組合せにスマートカードを設定し、「SMARTACCESS による Windows ログオン」を「する」に設定してください。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 **「設定項目一覧」から「ログオン認証」→「Windows ログオン」→「カードのポーリング動作」をクリックします。**

「カードのポーリング動作」の詳細が表示されます。

3 **「カードのポーリング動作」－「設定」の「する」をクリックします。**

4 **「動作」の「コンピュータをロックする」をクリックし、「OK」をクリックします。**

重要

- 「カードのポーリング動作」を「強制ログオフする」または「強制シャットダウンする」に設定している場合は、Windows のアクティブデスクトップ機能を利用しないでください。

スマートカードの利用

カードのポーリング動作を設定すると、スマートカードを利用して Windows ログオンした後は、スマートカードを抜き取るだけでコンピュータをロックすることができます。
コンピュータのロックを解除する場合は、【Ctrl】+【Alt】+【Delete】キーを押した後、スマートカードをセットして PIN を入力します。

3 BIOS 指紋認証による Windows ログオン

BIOS 指紋認証を利用すると、コンピュータの起動時に BIOS に登録されている指紋を使って認証します。またシングルサインオンを有効にすると、コンピュータの起動時の指紋認証のみで Windows を起動することもできます。

重要

- BIOS に指紋を登録するには、あらかじめ指紋のユーザーを登録し、さらに指紋を登録しておく必要があります。指紋を登録していないユーザーを BIOS に登録することはできません。
- ユーザー名は大文字小文字を区別します。BIOS へ登録するときに入力するユーザー名は指紋ユーザー名と一致するように入力してください。
- BIOS 指紋認証をお使いになるには、BIOS セットアップの起動時にパスワード入力を必要とするように設定する必要があります。
- 指紋で認証して BIOS セットアップを起動する場合は、BIOS セットアップの管理者ではなくユーザーとなります。BIOS セットアップの管理者として認証するためには、指紋ではなくパスワードによる認証を行う必要があります。「ユーザー認証方式」を「指紋認証のみ」に設定している環境で、管理者として BIOS セットアップを起動するためには、一度「指紋認証またはレガシーパスワード認証」に変更して再起動し、BIOS セットアップでの認証はパスワードで行うようにしてください。
- BIOS 指紋認証は BIOS 指紋認証機能に対応している機種のみで使用可能です。
- あらかじめ認証パターンの組合せに指紋を設定し、「SMARTACCESSによるWindowsログオン」を「する」に設定してください。

ここでは、「Windows ログオンとのシングルサインオン」、「BIOS 指紋ユーザーの新規登録」、「BIOS パスワードの有効化」の設定と利用について説明します。

BIOS 指紋認証の設定

BIOS 指紋認証を設定するには、「SMARTACCESS による Windows ログオン」を「する」に設定した後、BIOS シングルサインオンの有効化→ BIOS 指紋ユーザーの登録→ BIOS パスワードの有効化の順に設定を行います。

■BIOS シングルサインオンを有効にする

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ポリシー」→「BIOS」をクリックします。

「BIOS 認証」の詳細が表示されます。

3 **「Windowsログオンとのシングルサインオン」の「する」をクリックします。**

重要

- ご購入時のユーザー認証方式は「指紋認証またはレガシーパスワード認証」となっています。ユーザー認証方式が「指紋認証のみ」の場合、登録した指紋の品質が悪い場合や指にけがをしたときに、コンピュータにログオンできなくなることがありますのでご注意ください。

■BIOS 指紋ユーザーの登録

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が起動します。

2 **「ユーザー情報管理」→「BIOS」の順にクリックします。**

3 指紋認証画面が表示されるので、指紋を入力します。

「指紋ユーザー情報」が表示されます。

4 「指紋ユーザー情報」の「登録」をクリックします。

「指紋の登録」ウィンドウが表示されます。

5 「ユーザー名」に指紋でログオンする SMARTACCESS アカウントを入力します。

6 登録の確認後、「環境設定」で「OK」をクリックします。

■BIOS パスワードを有効にする

コンピュータを再起動し、BIOS 設定画面で起動時のパスワードを設定します。

重要

- BIOS セットアップの起動と設定は、お使いのコンピュータによって異なります。詳しくは、パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」をご覧ください。

BIOS 指紋を利用してログオン

BIOS 指紋認証を利用して、Windows を起動します。

1 コンピュータを起動します。

指紋認証画面が表示されます。

2 認証タイプで「指紋認証」を選択し、指紋を入力します。

重要

- BIOS 指紋認証では指紋の情報をBIOS 内に格納しています。BIOS 内に格納されている情報を削除する場合は「ユーザー情報管理」→「BIOS」から、指紋ユーザー情報を削除する必要があります。

POINT

- Windows ログオン時には「Windows へようこそ」の画面が表示されます。

第 7 章

困ったときには

おかしいなと思ったときや、わからないことがあったときの対処方法について説明しています。

1 セキュリティチップ

□ BIOS でセキュリティチップの設定を変更できない（FMV-W シリーズ以外の場合）

BIOS で、セキュリティチップの使用や、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

□ Infineon TPM Professional Package（Infineon Security Platform）ユーティリティがインストールできない

ソフトウェアをインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。
BIOS の設定については、パソコンまたはワークステーション本体の『製品ガイド』をご覧ください。

□ Windows ログオン時に機器が変更された旨のエラーメッセージが表示される

前回の起動からハードウェアの構成や設定が変更された可能性があります。ハードウェア構成や BIOS 設定など変更されていないか確認してください。変更があった場合は、機器を登録したときの状態に戻してください。
なお、変更の内容によっては、機器を登録したときの状態に戻しても、エラーメッセージが解除されない場合があります。詳しくは「認証デバイスについて」－「セキュリティチップ」－「機器監査について」（→ P.22）をご覧ください。

□ Windows ログオン時にユーザーキーパスワードエラーになる

SMARTACCESS による Windows ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

□ EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされていることが必要です。FAT32 のドライブでは EFS を利用することはできません。なお、Windows XP Home Edition では、EFS は利用できません。

□ セキュリティチップを「Disabled」（FMV-ESPRIMO、FMV FA パソコン、CELSIUS シリーズの場合）または「使用しない」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）に設定すると、Windows にログオンできなくなった

SMARTACCESS による Windows ログオンを設定した状態で、セキュリティチップを「Disabled」（FMV-ESPRIMO、FMV FA パソコン、CELSIUS シリーズの場合）または「使用しない」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）に設定すると、セキュリティチップに保存していた Windows パスワードが利用できず、Windows にログオンできなくなる場合があります。その場合はセキュリティチップを「Enabled」（FMV-ESPRIMO、FMV FA パソコン、CELSIUS シリーズの場合）または「使用する」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）に設定し直すか、「回避パスワード」でログオンする必要があります。
なお、「回避パスワード」でログオンしても、セキュリティチップで保護された環境は安全に管理されています。
回避パスワードについては『SMARTACCESS/Premium リファレンスガイド　機能編』または『SMARTACCESS/Basic リファレンスガイド　機能編』をご覧ください。

□ ハードウェア構成を変更したために Windows にログオンできなくなった

ハードウェアの構成を変更すると、SMARTACCESS の機器監査機能により Windows にログオンできなくなります。その場合はハードウェア構成を登録したときの設定に戻すか、機器構成を登録しなおす必要があります。設定方法については、次のマニュアルをご覧ください。

・SMARTACCESS/Premium をお使いの場合
　『SMARTACCESS/Premium リファレンスガイド　機能編』の「Windows ログオン」－「機器監査」
・SMARTACCESS/Basic をお使いの場合
　『SMARTACCESS/Basic リファレンスガイド　機能編』の「Windows ログオン」－「機器監査」

□ リストアを行うとユーザーキーパスワードが変わることがある

「認証デバイスについて」－「セキュリティチップ」－「リストアについて」（→ P.21）に従ってリストアを行った場合、ユーザーキーパスワードには、バックアップを行った時点でのパスワードが設定されます。
そのため、バックアップ後にユーザーキーパスワードを変更しても、復元すると、バックアップを行った時点でのパスワードに戻ります。

□ ソフトウェアのインストール時に「アプリケーションエラー」が表示されることがある

「インストールと設定」（→ P.47）の手順に従ってソフトウェアをインストールしない場合、「アプリケーションエラー」が表示されることがあります。
もし表示された場合、ソフトウェアのインストールを引き続き行い、インストール終了後は表示画面に従って Windows を再起動してください。再起動後は正常に動作します。

□ SMARTACCESS でユーザ初期化を行うと、失敗することがある

SMARTACCESS をインストール時に、セキュリティチップがクリアされていない状態で行うと、ユーザ初期化に失敗することがあります。インストール時にはセキュリティチップがクリアされていたかどうか確認してください。クリアされていなかった場合にはSMARTACCESS をアンインストールし、BIOS でセキュリティチップをクリアした後、再度SMARTACCESS をインストールしてください。

2 指紋センサー

□ 指紋登録時にエラー表示される

・指の置き方が正しいか確認してください。指が正しく置かれていない、または、指を置く方向が毎回ずれていると登録できないことがあります（→「認証デバイスについて」－「指紋センサー」－「使い方」（→ P.28）。
・指が乾燥していませんか。
手を洗う、指に息を吹きかけるなど指がしっとりする程度の湿り気を与えることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「使用上のご注意」（→ P.26）。
・指が濡れていませんか。
乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「使用上のご注意」（→ P.26）。
・センサー表面を確認してください。汚れていたり、汗などの水分が付着していると指紋が読み取れない場合があります（→「認証デバイスについて」－「指紋センサー」－「使用上のご注意」（→ P.26）。
・異なる指で再度登録してください。

□ 指紋照合時にエラー表示される

・指の置き方が正しいか確認してください。指が正しく置かれていないと照合できないことがあります（→「認証デバイスについて」－「指紋センサー」－「使い方」（→ P.28）。
・指が乾燥していませんか。
手を洗う、指に息を吹きかけるなど指がしっとりする程度の湿り気を与えることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「使用上のご注意」（→ P.26）。
・指が濡れていませんか。
乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「使用上のご注意」（→ P.26）。
・センサー表面を確認してください。汚れていたり、汗などの水分が付着していると指紋が読み取れない場合があります（→「認証デバイスについて」－「指紋センサー」－「使用上のご注意」（→ P.26）。
・登録したもう片方の指で照合してください。

3 FeliCa 対応リーダ／ライタ

□ FeliCa 対応非接触 IC カードを使って Windows ログオンを行っている場合、BIOS セットアップの「FeliCa デバイス」の設定を「使用しない」にすると、Windows にログオンできなくなる

FeliCa 対応非接触 IC カードを使って Windows ログオンを行っている場合は、BIOS セットアップの「FeliCa デバイス」の設定を「使用する」にしてください。BIOS セットアップの設定については、パソコン本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧ください。

□ SMARTACCESS/Premium を利用している場合、FeliCa リーダー / ライターソフトウェアをアンインストールすると、Windows が起動できなくなる

FeliCaリーダー /ライターソフトウェアをアンインストールする場合は、SMARTACCESS/Premiumをアンインストールした後で行ってください。

FeliCaリーダー /ライターソフトウェアがインストールされていない状態でSMARTACCESS/PremiumによるログオンをうとWindowsが正常に起動できなくなります。

Windowsが正常に起動できなくなった場合は、「富士通ハードウェア修理相談センター」、またはご購入元にお問い合わせください。

4 スマートカードリーダ／ライタ、スマートカードホルダー

スマートカードリーダ／ライタ、およびスマートカードホルダーをお使いのときに表示されるエラーメッセージについては、パソコンまたはワークステーション本体の『製品ガイド』の「BIOS」－「セキュリティ機能を使うには」をご覧ください。

5 SMARTACCESS

SMARTACCESSをお使いのときのトラブルや、エラーメッセージが表示されたときの対処方法については、『SMARTACCESS/Premiumリファレンスガイド ツール編』または『SMARTACCESS/Basicリファレンスガイド ツール編』の「トラブルシューティング」をご覧ください。

SMARTACCESS ファーストステップガイド
（認証デバイスをお使いになる方へ）

B6FH-9831-01 Z2-00

発 行 日　2006 年 4 月
発行責任　富士通株式会社